BITCOIN (A BASIC TUTORIAL)

Aviv Zohar

The Rachel & Selim Benin School of Eng. and Computer Science
The Hebrew University

In this tutorial:

- What is Bitcoin and how does is work?
- What are the main challenges?
- The surrounding ecosystem
- Pointers to related research & additional sources of information

THE TOOTH FAIRY LEFT ME... BITCOINS?!
WASSERMAN ©2.14
DIST. BY TRIBUNE CONTENT AGENCY
www.bostonglobe.com/wasserman

Money isn’t perfect

Currently slower and more expensive than:

A decentralized digital currency

Invented by Satoshi Nakamoto in 2008
Launched in 2009

Built for the age of the internet

Features of Bitcoin

Pseudonymous

Fixed amount

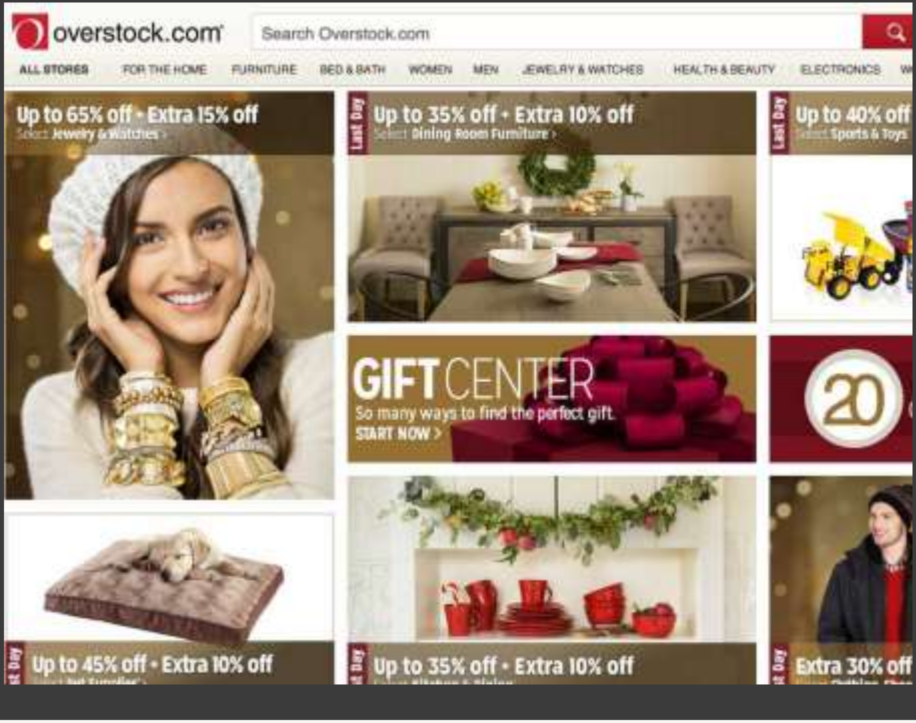
Irreversible Transfers

Cannot be seized

Can not be frozen

Escrow

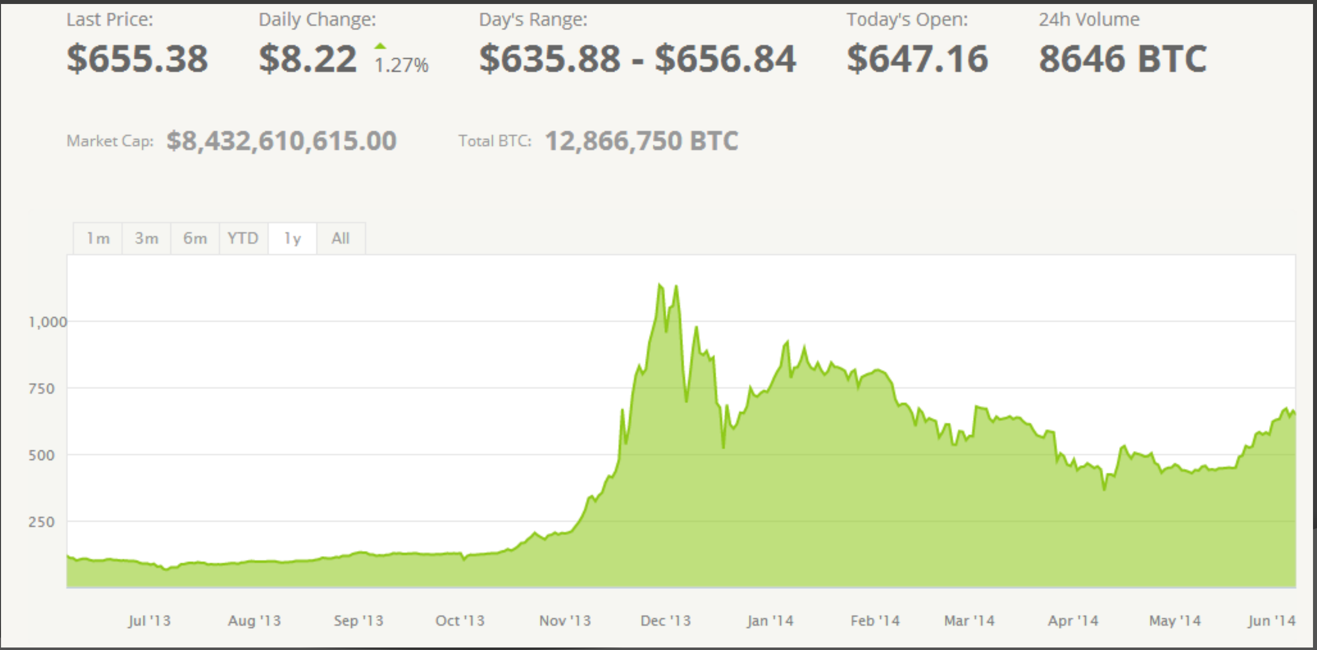
Joint accounts



coinbase

bitpay

CIRCLE

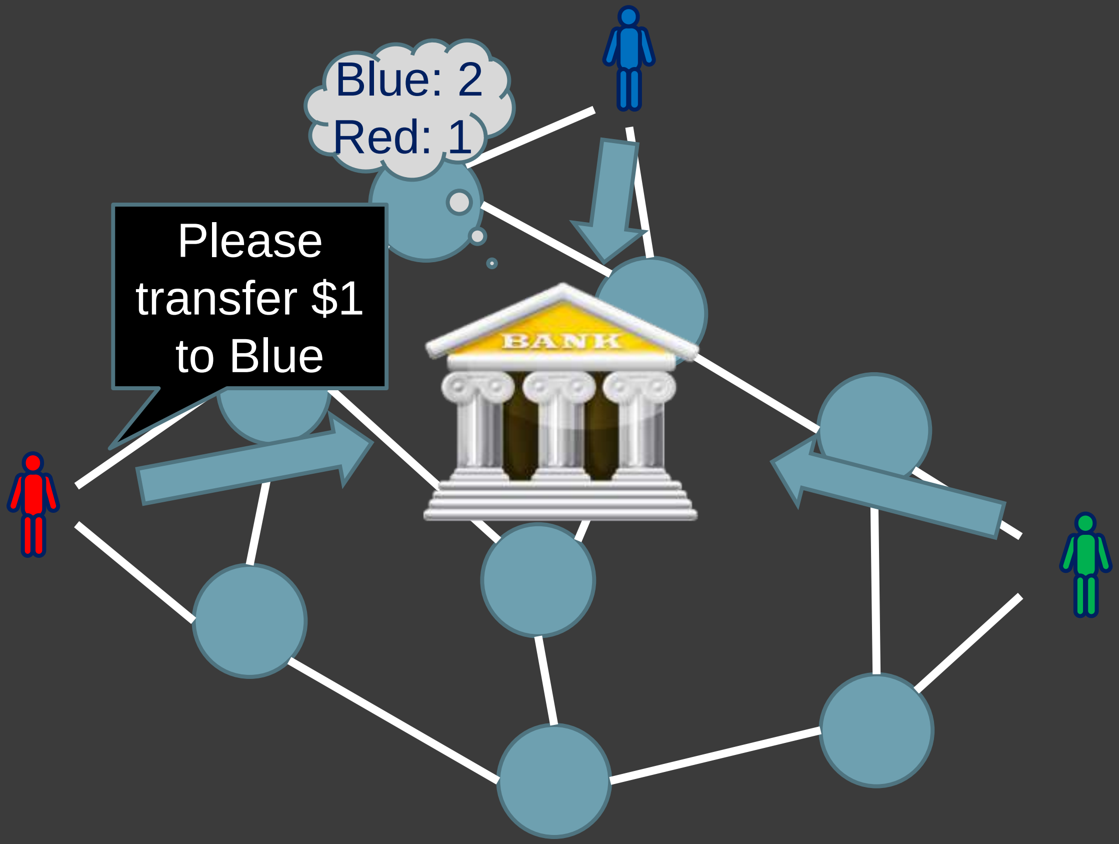


Last Price:	Daily Change:	Day's Range:	Today's Open:	24h Volume
$655.38	$8.22 1.27%	$635.88 - $656.84	$647.16	8646 BTC

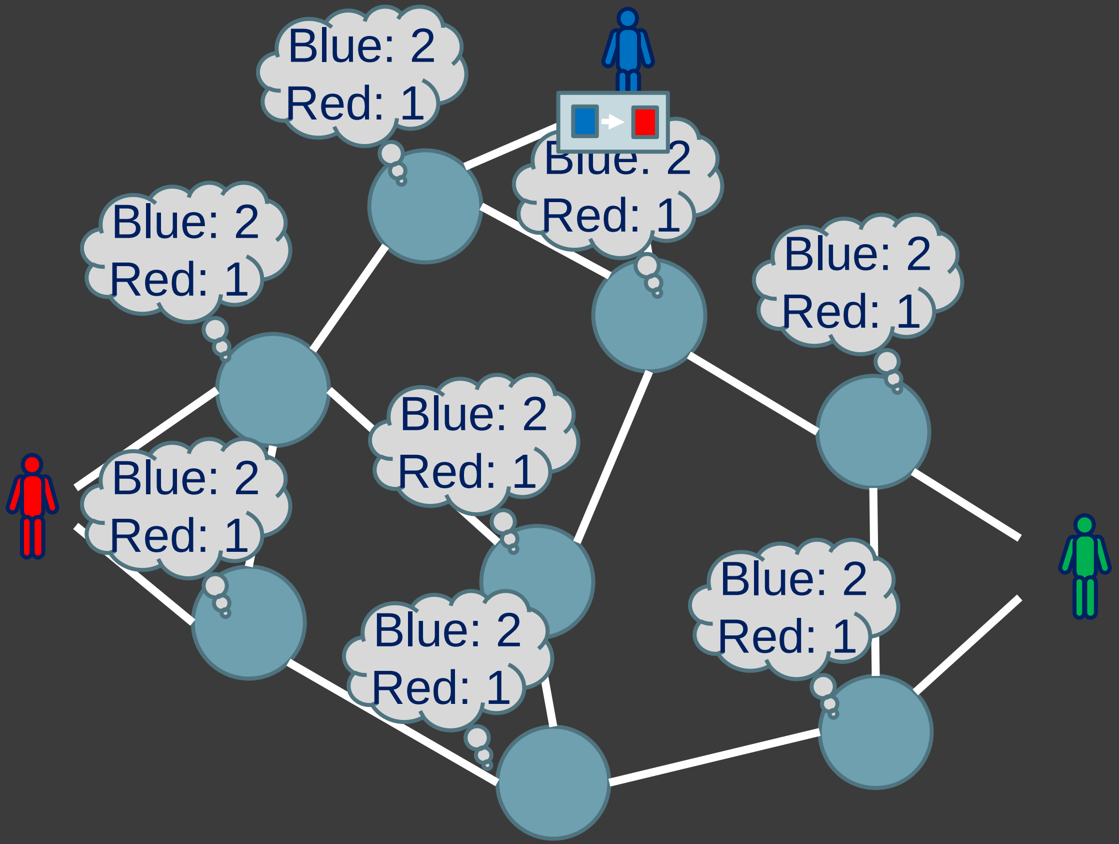
Market Cap: $8,432,610,615.00

Total BTC: 12,866,750 BTC

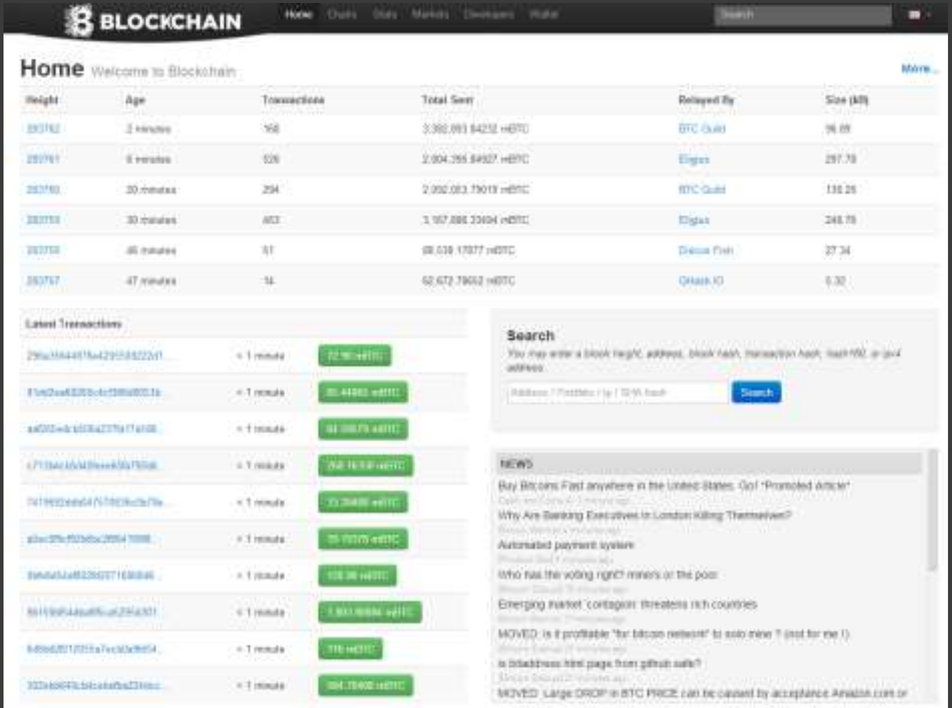
*From Bitstamp.net



- Bypass regulation & censorship
- Increase competition
- Disrupt


Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1
Blue: 2 Red: 1

Transactions are thus public, addresses are (free) pseudonyms



Home Welcome to Blockchain

More...

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
283762	2 minutes	168	3,392,093.84232 mBTC	BTC Guild	96.89
283761	6 minutes	526	2,004,356.84927 mBTC	Eligius	297.79
283760	20 minutes	294	2,092,083.79019 mBTC	BTC Guild	138.26
283759	30 minutes	463	3,167,886.33404 mBTC	Eligius	248.79
283758	46 minutes	51	88,038.17077 mBTC	Discus Fish	27.34
283757	47 minutes	14	62,672.79652 mBTC	GHash.IO	6.32

Latest Transactions

29fa[illegible]...	< 1 minute	72.90 mBTC
f1eb2[illegible]...	< 1 minute	30.44863 mBTC
aa0[illegible]...	< 1 minute	[illegible] mBTC
c71[illegible]...	< 1 minute	[illegible] mBTC
7419[illegible]...	< 1 minute	[illegible] mBTC
a3ec[illegible]...	< 1 minute	[illegible] mBTC
8a[illegible]...	< 1 minute	108.38 mBTC
8611[illegible]...	< 1 minute	1,[illegible] mBTC
6d[illegible]...	< 1 minute	116 mBTC
332[illegible]...	< 1 minute	[illegible] mBTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address.

Address / Firstbits / Ip / SHA hash [Search]

NEWS

Buy Bitcoins Fast anywhere in the United States. Go! *Promoted Article*

Why Are Banking Executives In London Killing Themselves?

Automated payment system

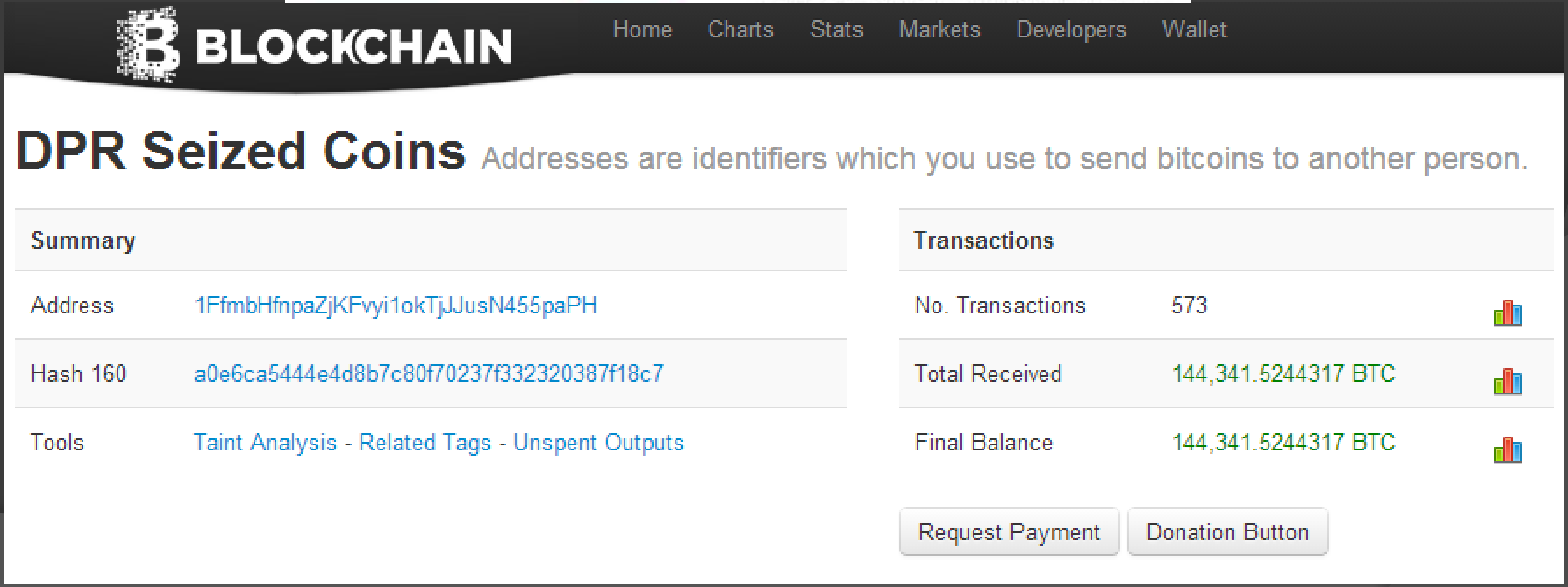
Who has the voting right? miners or the pool

Emerging market 'contagion' threatens rich countries

MOVED: Is it profitable "for bitcoin network" to solo mine ? (not for me !)

is bitaddress html page from github safe?

MOVED: Large DROP in BTC PRICE can be caused by acceptance Amazon.com or

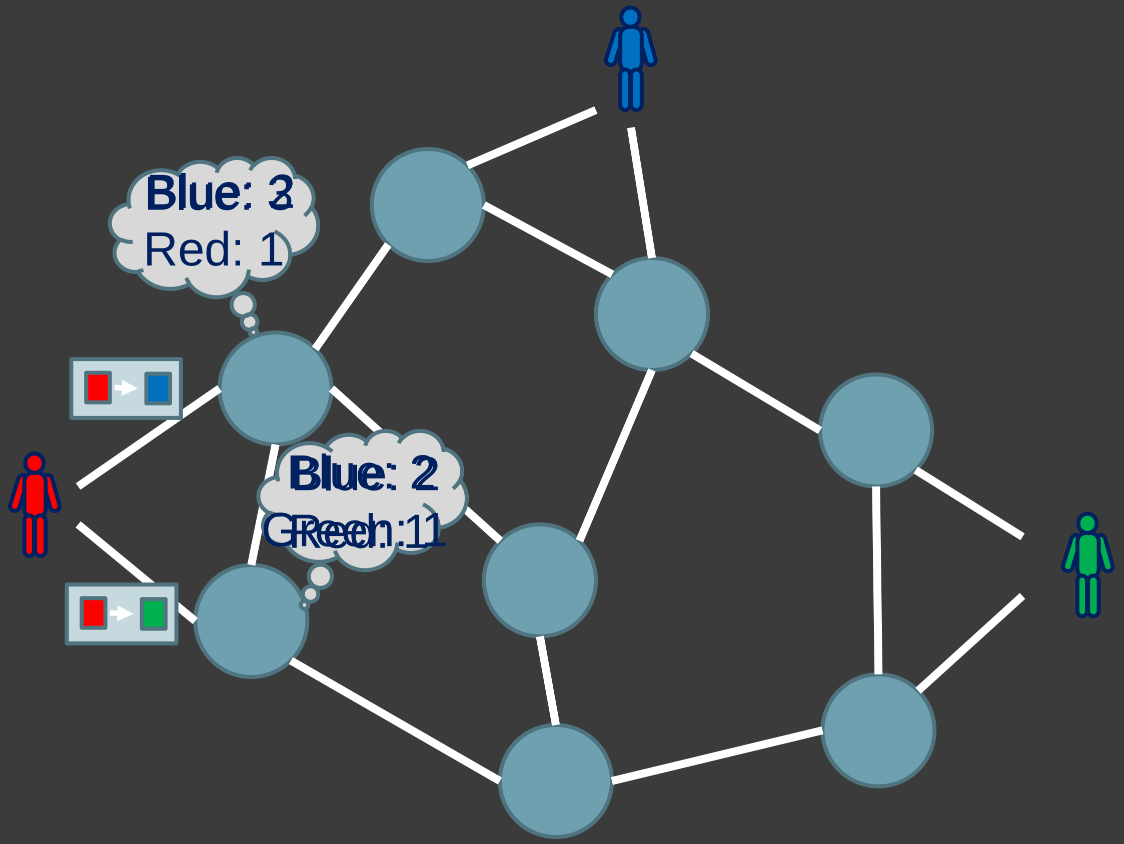


DPR Seized Coins Addresses are identifiers which you use to send bitcoins to another person.

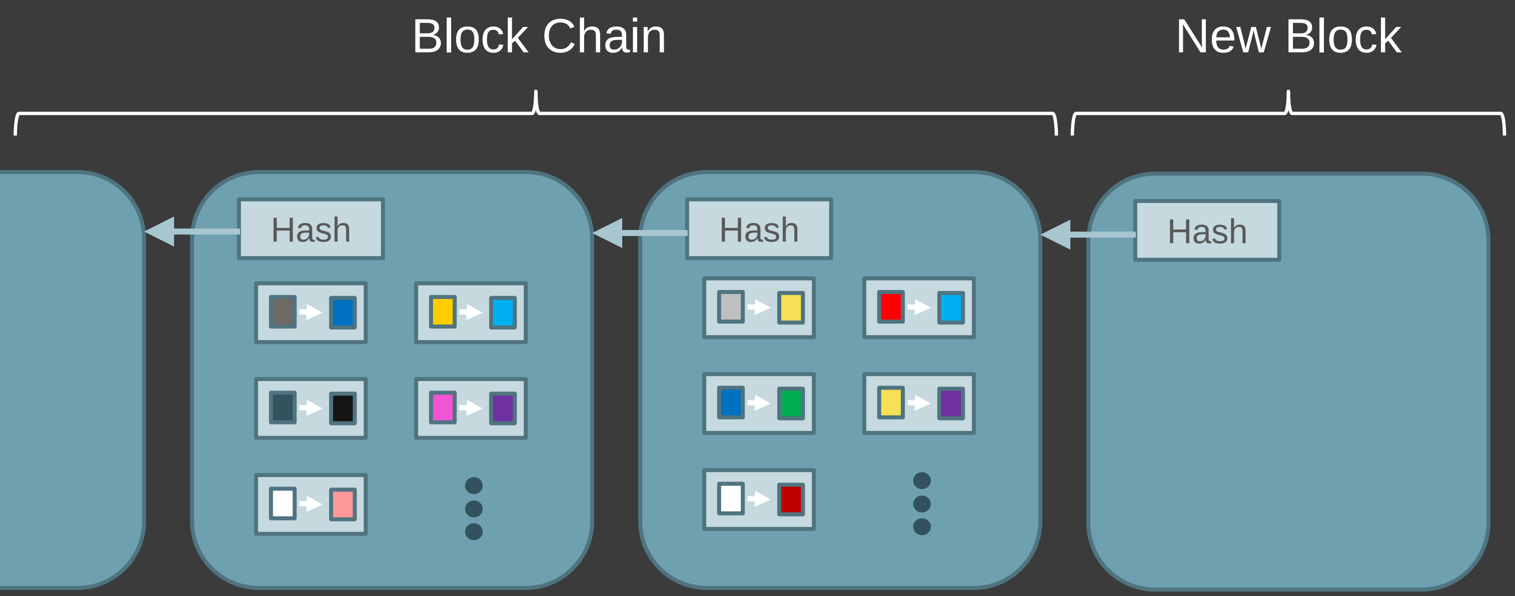
Summary	
Address	1FfmbHfnpaZjKFvyi1okTjJJusN455paPH
Hash 160	a0e6ca5444e4d8b7c80f70237f332320387f18c7
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions		
No. Transactions	573	📊
Total Received	144,341.5244317 BTC	📊
Final Balance	144,341.5244317 BTC	📊

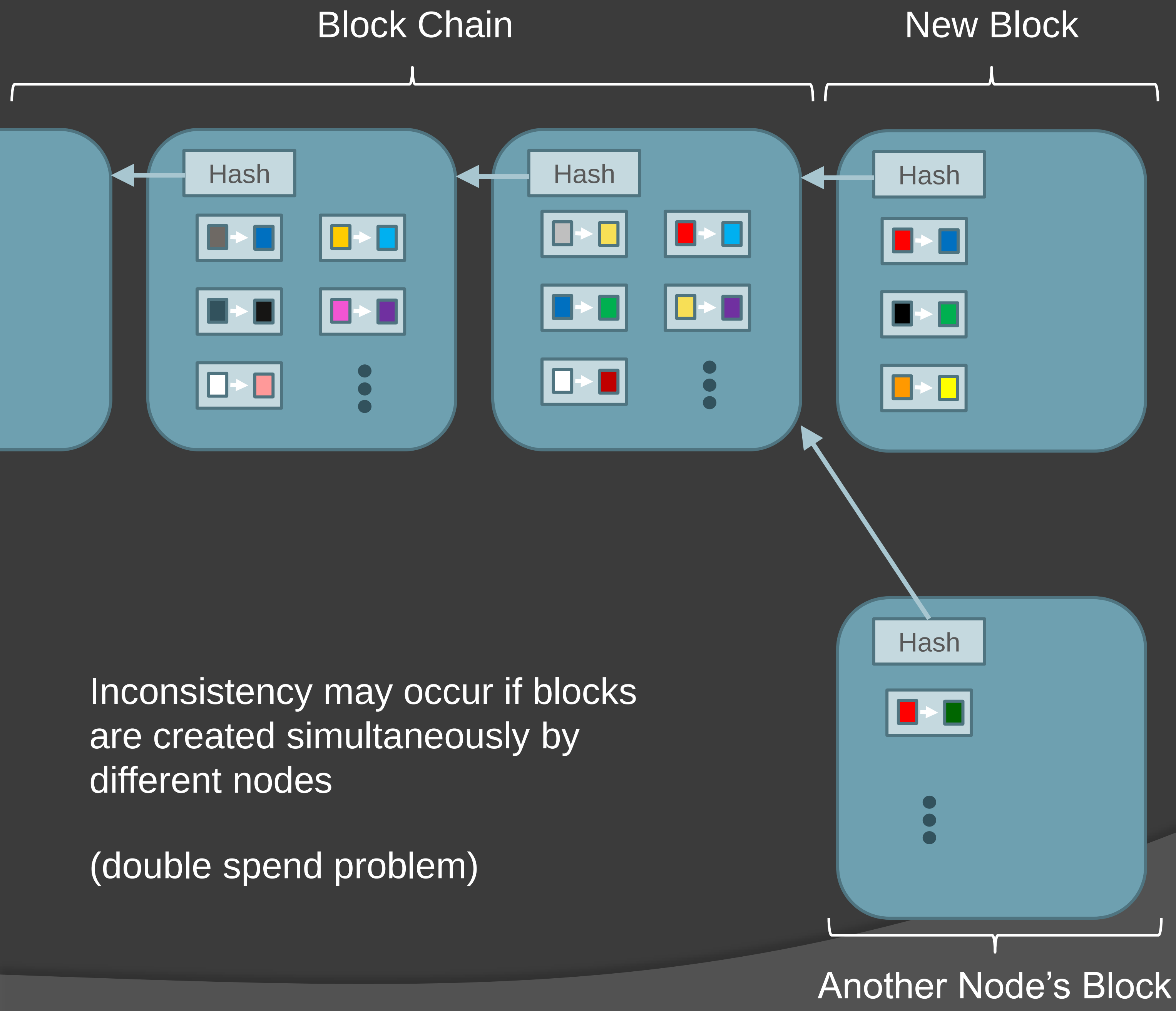
The Double-spend problem



A variant of the Byzantine general’s problem (Byzantine consensus in asynchronous dist. systems)

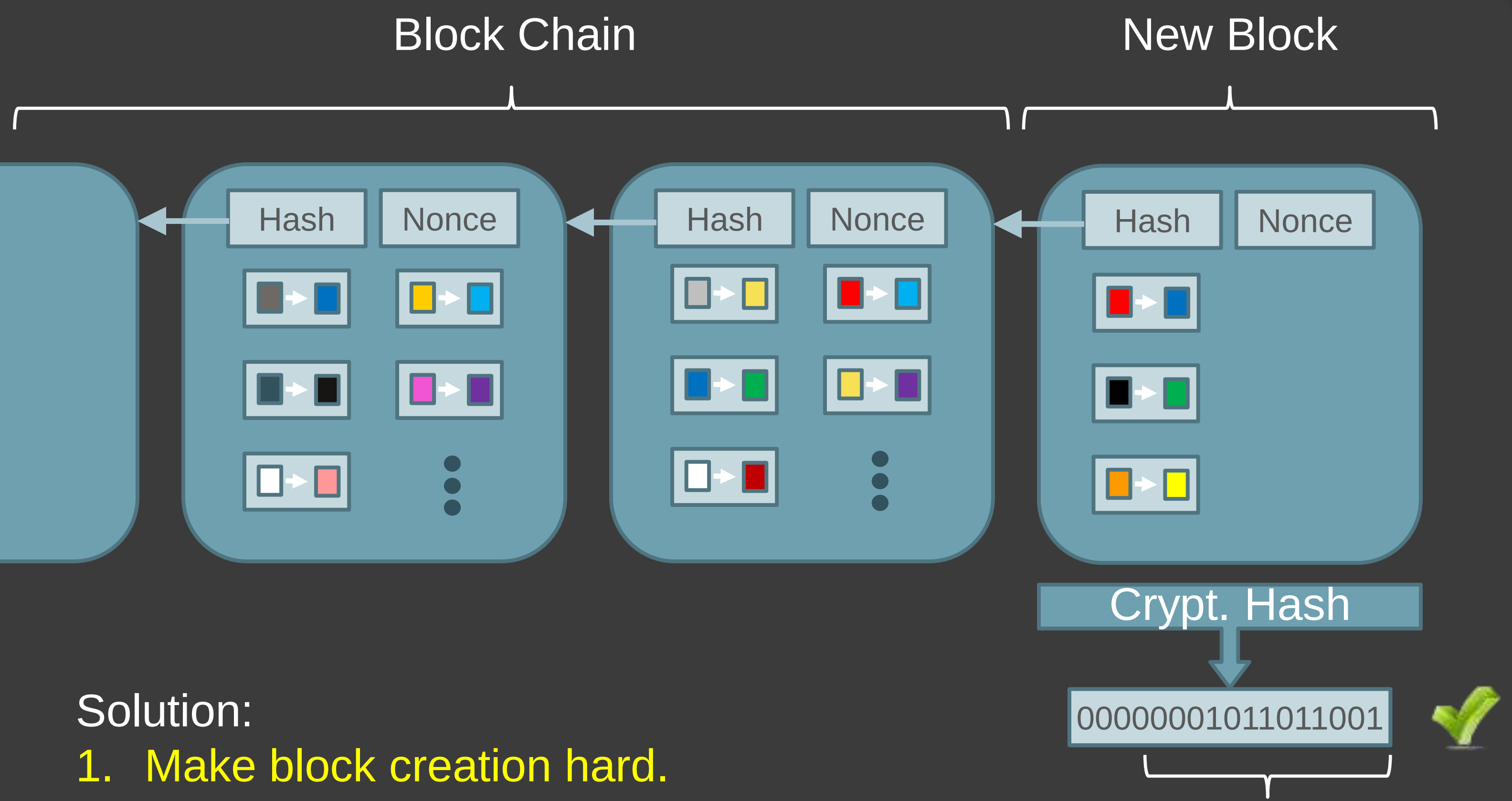


- Blocks aggregate transactions in batches
- Each block contains a cryptographic hash of the prev one, “proving” it is created afterwards.
- Can Read ledger from start to finish to “follow the money”
- Each node tries to grow the chain with recent transactions:
  - Create a block with recent consistent transactions
  - Send to peers



Inconsistency may occur if blocks are created simultaneously by different nodes

(double spend problem)



Solution:

1. Make block creation hard.
2. Adopt conflicting blocks if they make up a longer chain.

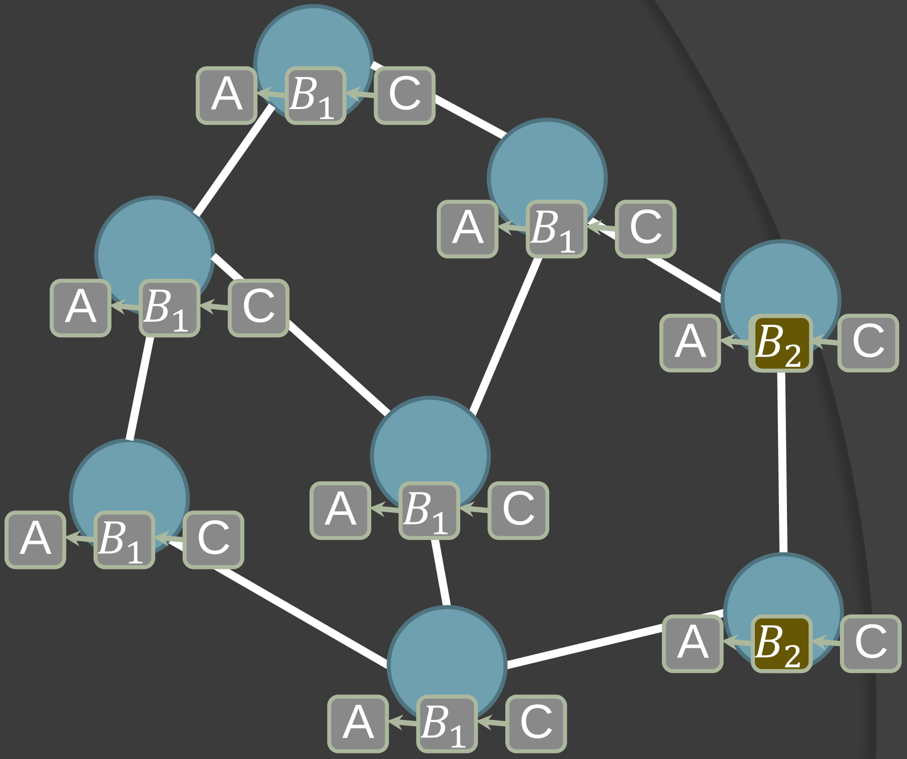
Must be a small number for valid block
(under some target value)

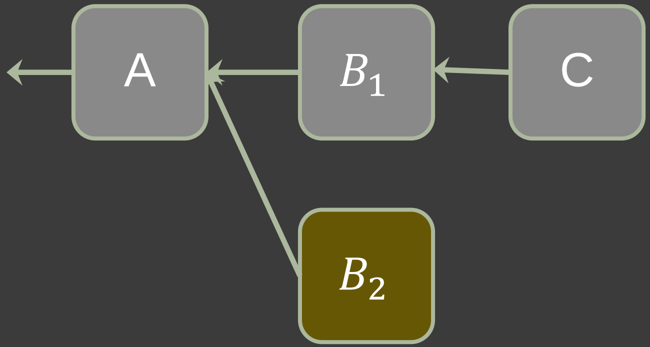
If not, change Nonce & try again

~ one block per 10 min. in the entire network
(Difficulty scales automatically to maintain this)
Current traget has ~65 zeros in most significant digits

1. Make block creation hard (once every 10 minutes)

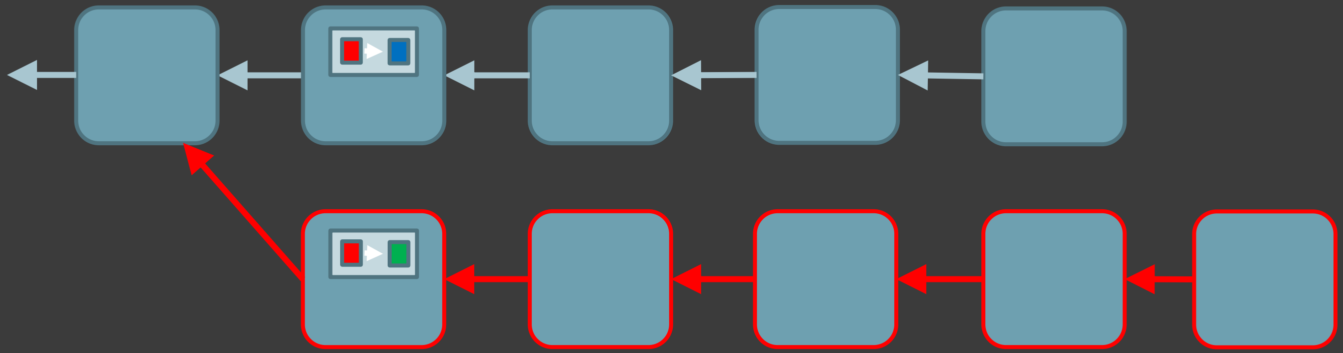
2. Adopt (conflicting) blocks iff they make up a longer chain.





The Double-Spend Attack

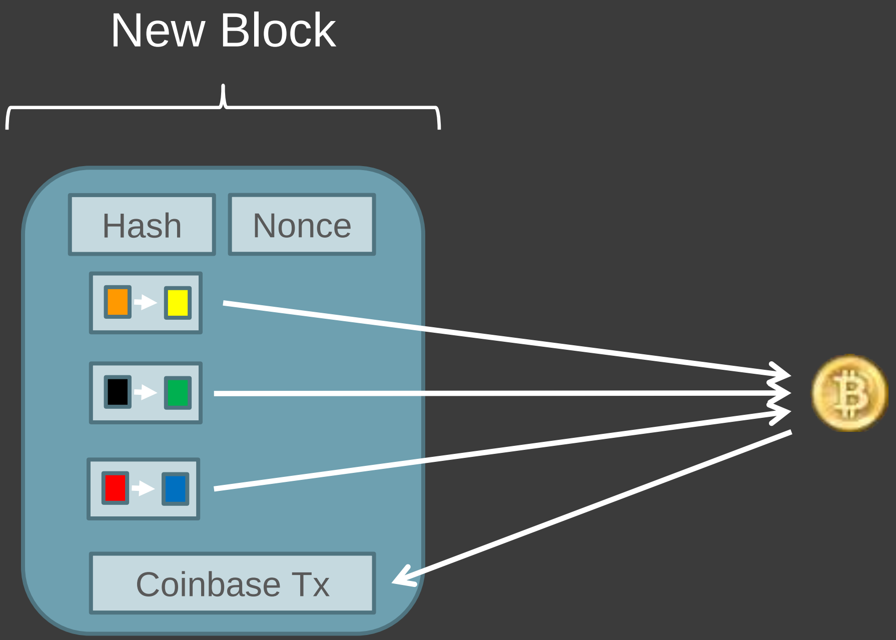
- A payment can be reversed!
- Easy if attacker has >50% of compute power
- Possible with less than 50%



Bitcoin's Guarantee [Satoshi]:

If attacker controls < 50% of compute power, probability of block replacement decreases exponentially with time.

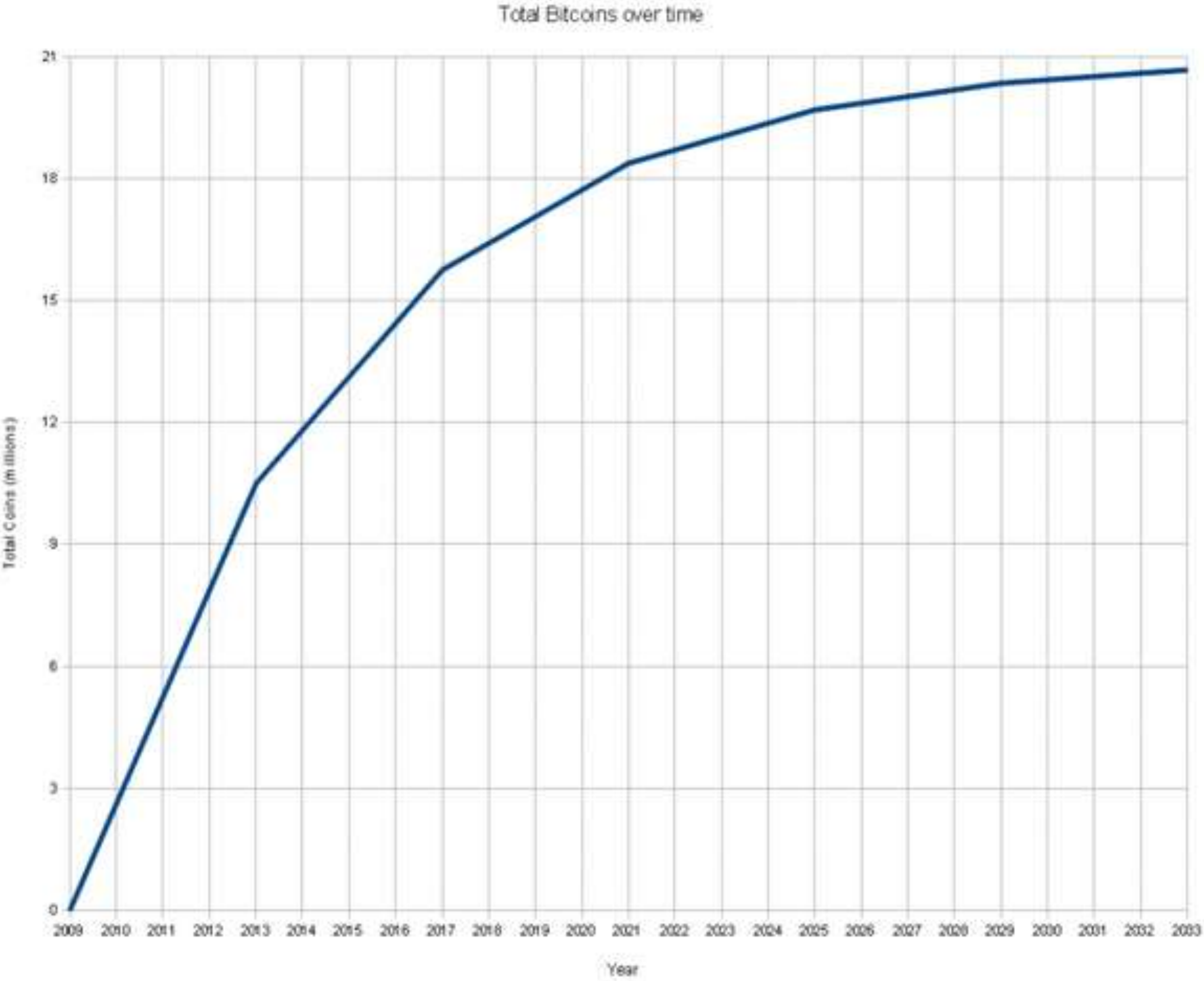
To encourage nodes to authorize transactions:



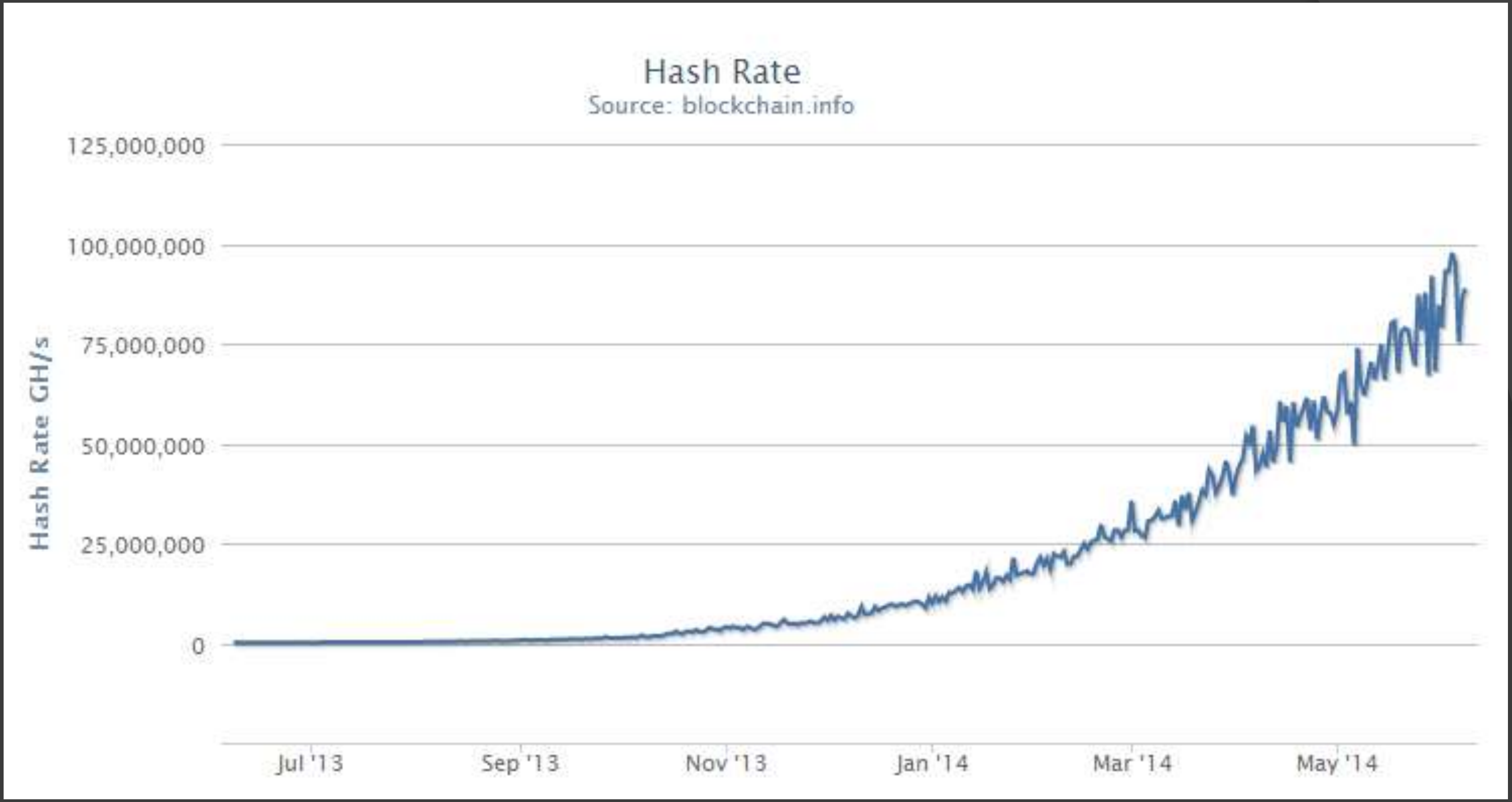
Reward the authorizer with fees from each transaction (+ newly minted money)

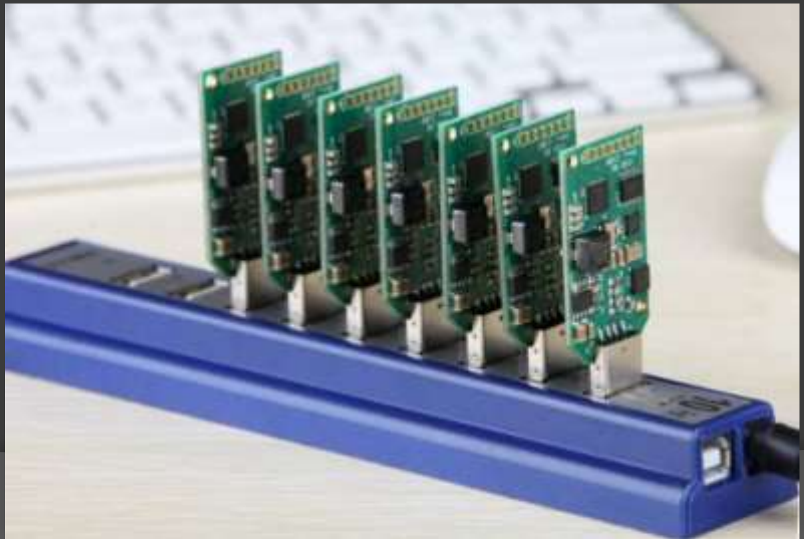
Block creation is known as “Mining”

Block size is limited (currently to 1MB)
Transactions will compete to enter – highest fee first.
(An auction!)



Total Bitcoins over time
Total Coins (millions)
21
18
15
12
9
6
3
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
Year


Hash Rate
Source: blockchain.info
Hash Rate GH/s
125,000,000
100,000,000
75,000,000
50,000,000
25,000,000
0
Jul '13
Sep '13
Nov '13
Jan '14
Mar '14
May '14

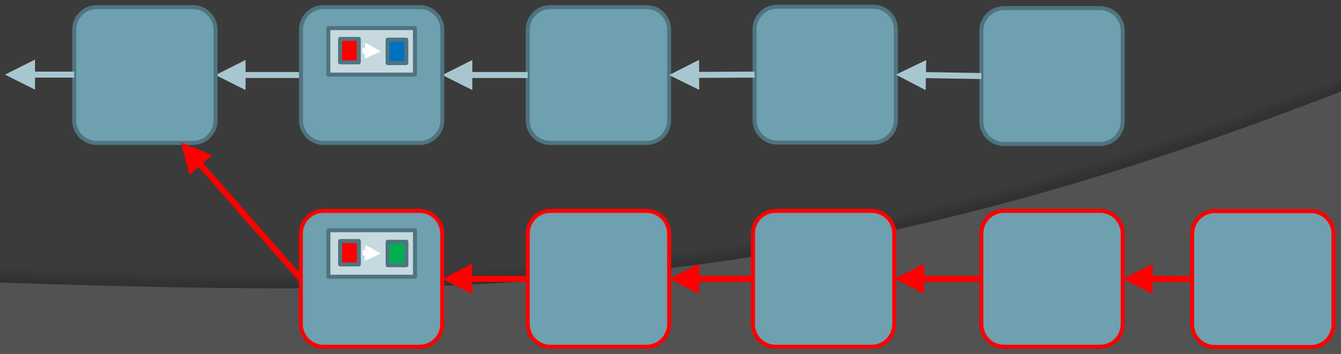


Attacks

Analysis of the Double Spend Attack

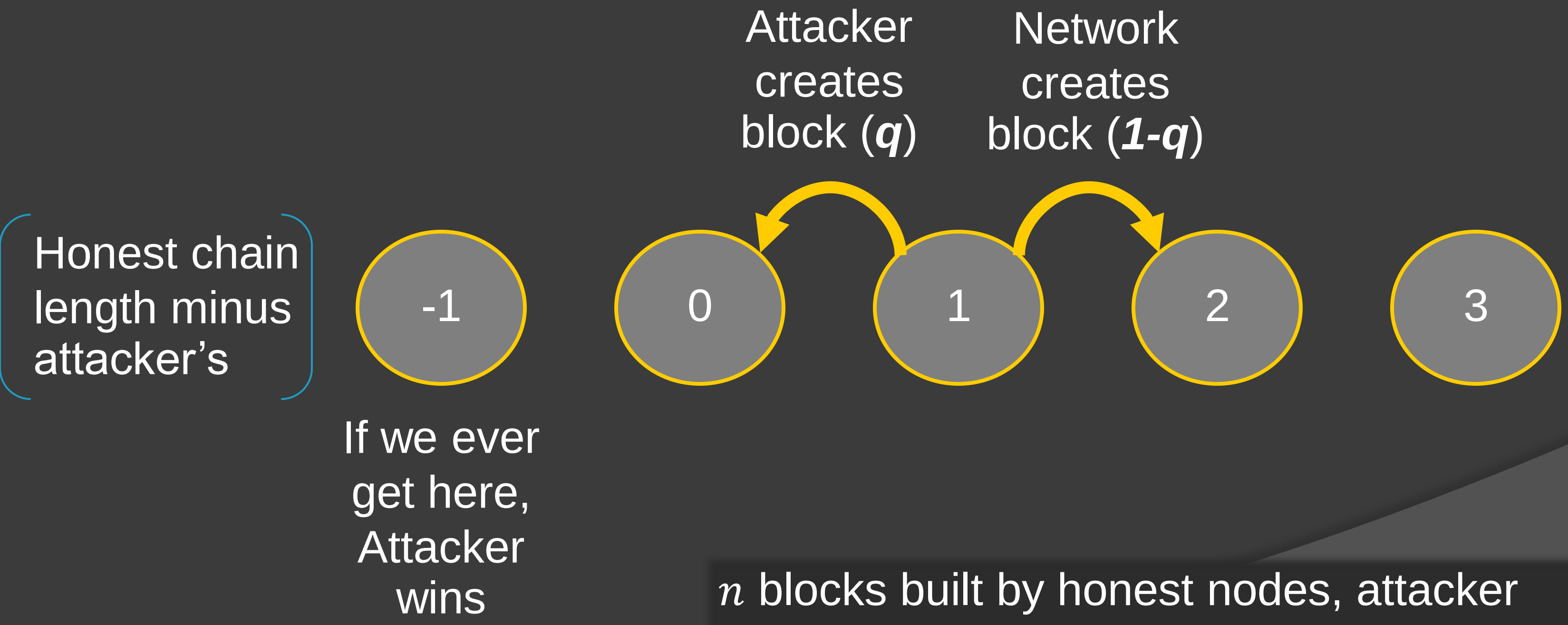
The recipient has an acceptance strategy:

- # of “confirmations” (blocks) it waits for before transaction is considered “accepted”.
- Assumption: attacker has hashrate q. Yields distribution over the # of blocks in its chain.



Analysis of the Attack

- Consider a Markov Process representing the difference in length between the chains


Attacker creates block (***q***)
Network creates block (***1-q***)
Honest chain length minus attacker's
-1
0
1
2
3
If we ever get here, Attacker wins

n blocks built by honest nodes, attacker has strength q → probability distribution over initial states $\in \{n, n-1, n-2, \ldots\}$.

The Result:

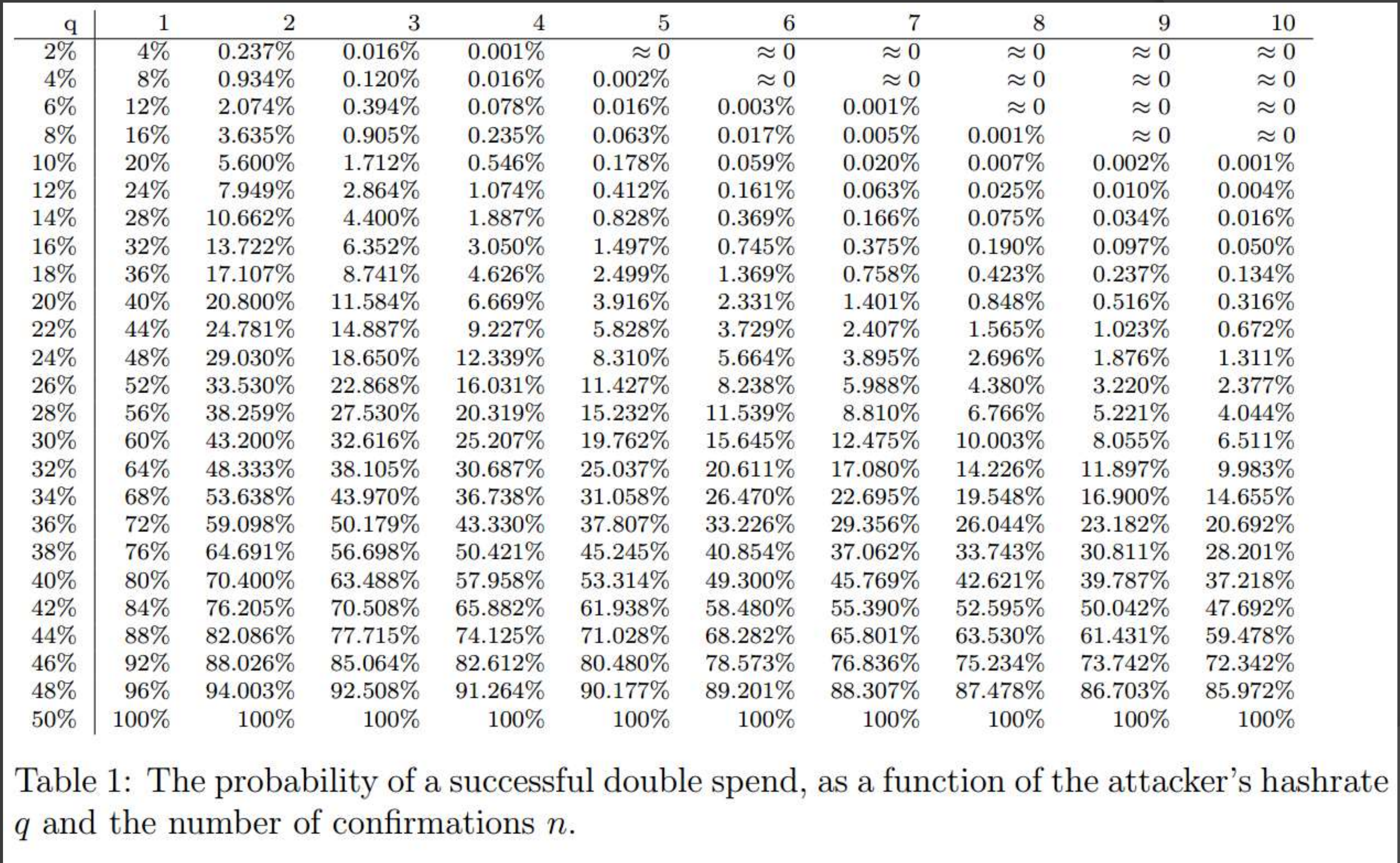
Attacker's strength: $q < 0.5$

Receiver's policy: wait for n confirmations

Probability of successful attack:

$$r = 1 - \sum_{m=0}^{n} \binom{m+n-1}{m} \cdot \left((1-\mathrm{q})^{\mathrm{n}}\mathrm{q}^{\mathrm{m}} - (1-\mathrm{q})^{\mathrm{m}}\mathrm{q}^{\mathrm{n}}\right)$$

Result due to Meni Rosenfeld: "Analysis of hashrate-based double-spending"



q	1	2	3	4	5	6	7	8	9	10
2%	4%	0.237%	0.016%	0.001%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
4%	8%	0.934%	0.120%	0.016%	0.002%	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
6%	12%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	≈ 0	≈ 0	≈ 0
8%	16%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	≈ 0	≈ 0
10%	20%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

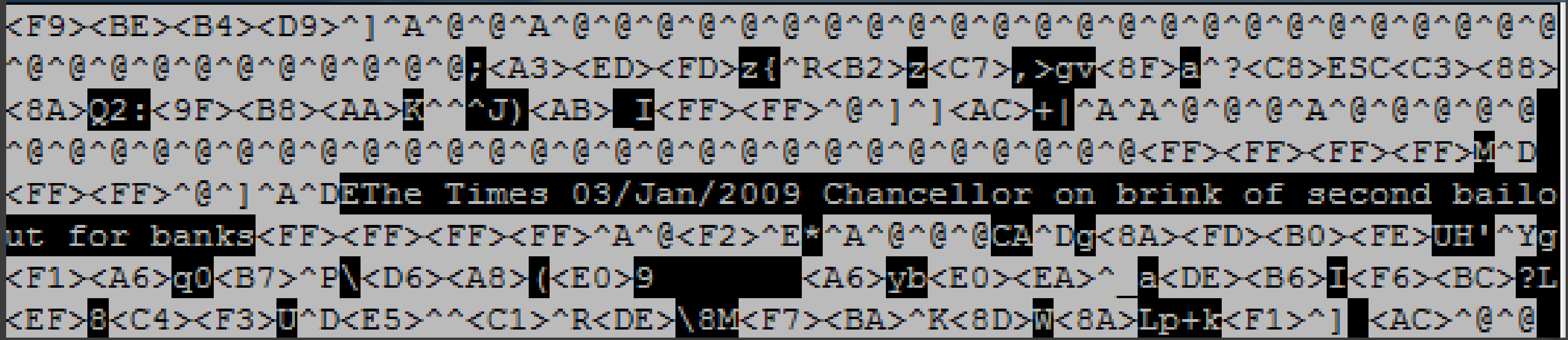
Table 1: The probability of a successful double spend, as a function of the attacker's hashrate q and the number of confirmations n.

From Meni Rosenfeld's paper "Analysis of hash-rate based double spending".

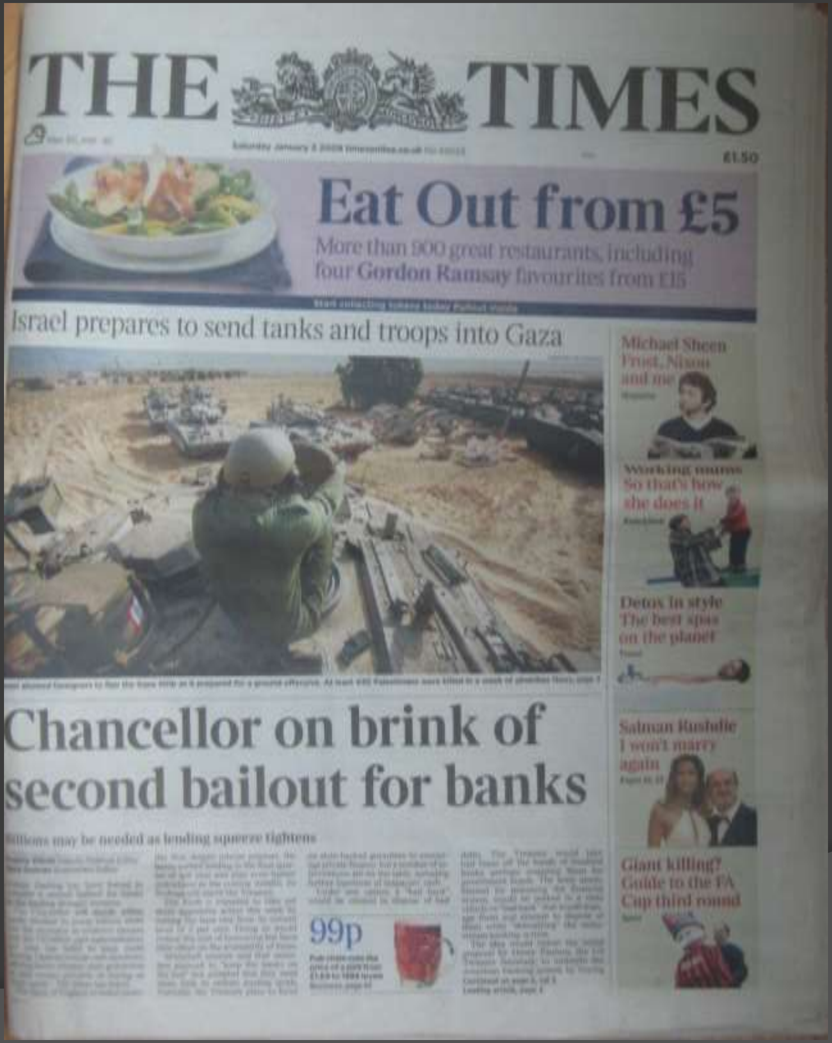
Implications

- To get final approval for a transaction one has to wait several blocks (confirmations).
- Each block takes 10 minutes in expectation.

Risk of an attack should take transaction size into account.



```
<F9><BE><B4><D9>^]^A^@^@^A^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@;<A3><ED><FD>z{^R<B2>z<C7>,>gv<8F>a^?<C8>ESC<C3><88>
<8A>Q2:<9F><B8><AA>K^^^J)<AB>_I<FF><FF>^@^]^]<AC>+|^A^A^@^@^@^A^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@<FF><FF><FF><FF>M^D
<FF><FF>^@^]^A^DEThe Times 03/Jan/2009 Chancellor on brink of second bailo
ut for banks<FF><FF><FF><FF>^A^@<F2>^E*^A^@^@^@CA^Dg<8A><FD><B0><FE>UH'^Yg
<F1><A6>q0<B7>^P\<D6><A8>(<E0>9       <A6>yb<E0><EA>^_a<DE><B6>I<F6><BC>?L
<EF>8<C4><F3>U^D<E5>^^<C1>^R<DE>\8M<F7><BA>^K<8D>W<8A>Lp+k<F1>^] <AC>^@^@
```



THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

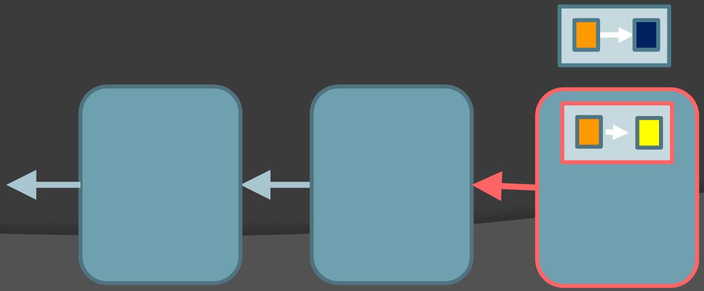
99p

The Finney attack

Some Vendors cannot afford to wait.
Accept 0-confirmation transactions.

Susceptible to a simple attack:

- Alice pre-mines block with a transaction to self.
- Alice creates and sends transaction paying bob. Instantly receives goods from Bob.
- Alice release pre-mined block before the transaction to Bob is authorized.



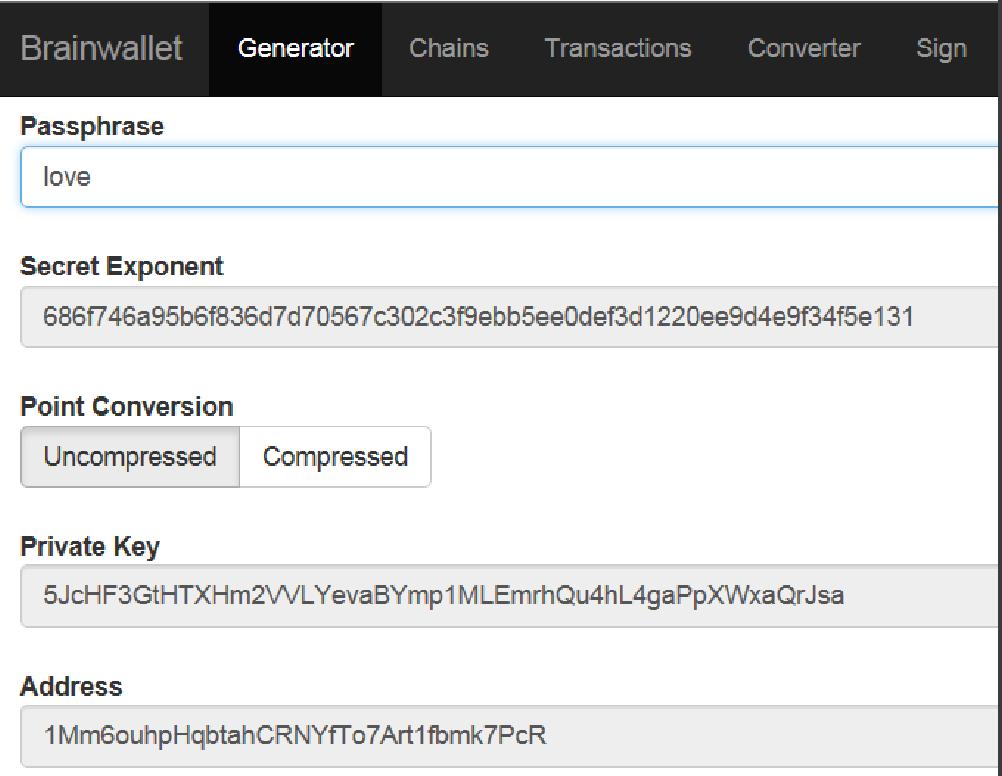
Additional Attack Vectors

- Network-structure attacks
  - Isolating a node implies you can use its computational power to launch double spend attacks
  - Sybil attacks
- DDoS attacks with amplification
  - Blocks are secure by difficulty, blocks that are too old are not allowed
  - Transactions are secured by fee
- Clock Drift attacks (Timejacking)
- 0-Confirmation attacks & chain splits based on different versions

Transactions

Addresses

- Addresses are (essentially) public keys
- Allow sending Bitcoins even when recipient is offline
- Signatures are used to prove ownership (generated with private keys)
- Security matters! paper wallets / cold storage.



Passphrase

love

Secret Exponent

686f746a95b6f836d7d70567c302c3f9ebb5ee0def3d1220ee9d4e9f34f5e131

Point Conversion

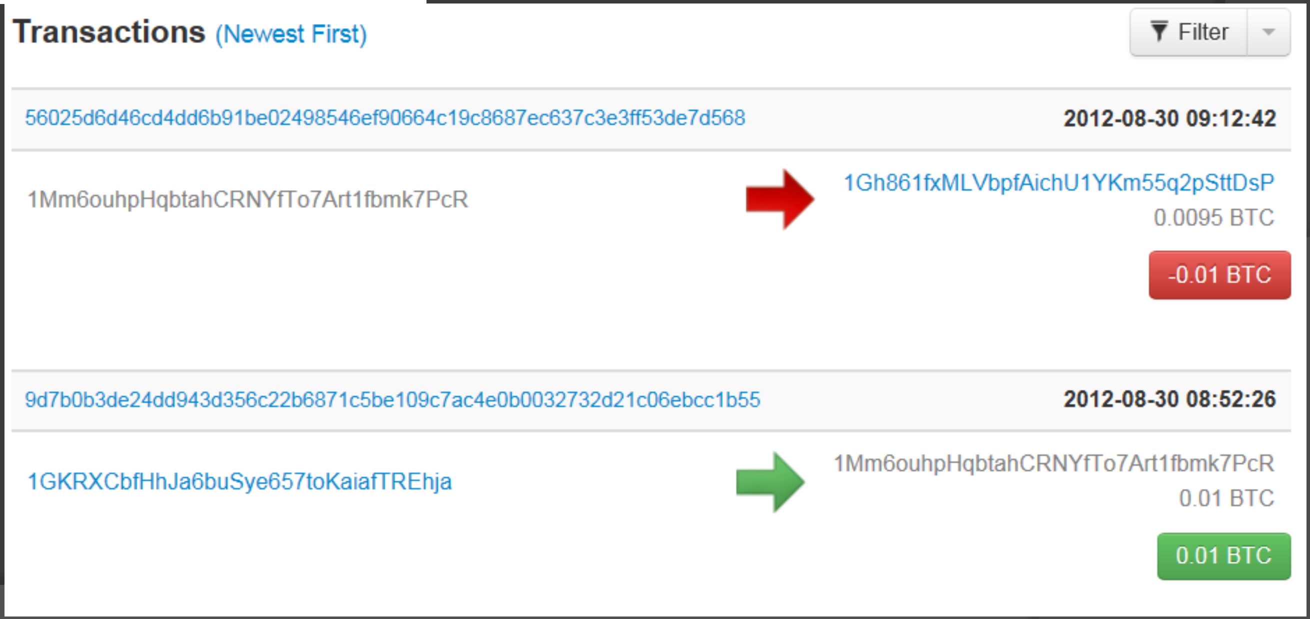
[✓ Uncompressed] Compressed

Private Key

5JcHF3GtHTXHm2VVLYevaBYmp1MLEmrhQu4hL4gaPpXWxaQrJsa

Address

1Mm6ouhpHqbtahCRNYfTo7Art1fbmk7PcR



Transactions (Newest First)

56025d6d46cd4dd6b91be02498546ef90664c19c8687ec637c3e3ff53de7d568 **2012-08-30 09:12:42**

1Mm6ouhpHqbtahCRNYfTo7Art1fbmk7PcR → 1Gh861fxMLVbpfAichU1YKm55q2pSttDsP 0.0095 BTC

-0.01 BTC

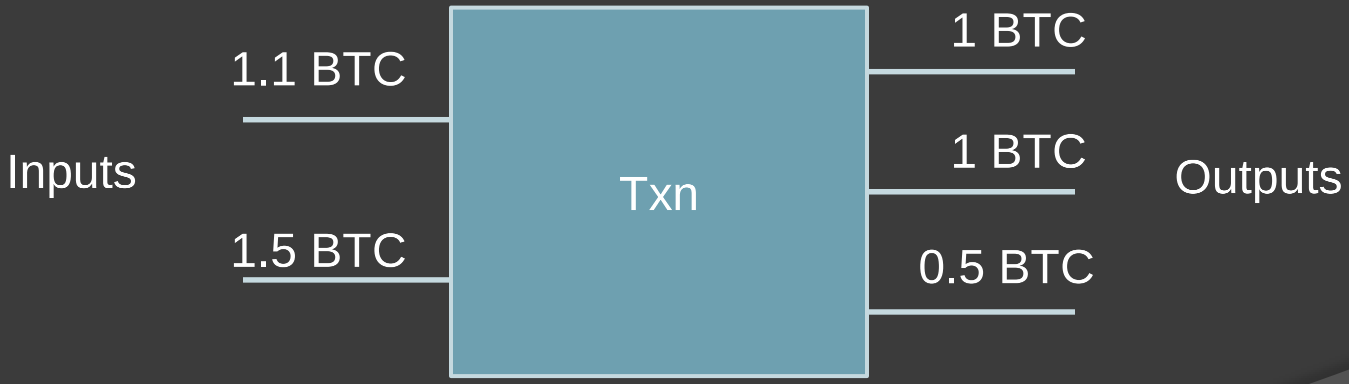
9d7b0b3de24dd943d356c22b6871c5be109c7ac4e0b0032732d21c06ebcc1b55 **2012-08-30 08:52:26**

1GKRXCbfHhJa6buSye657toKaiafTREhja → 1Mm6ouhpHqbtahCRNYfTo7Art1fbmk7PcR 0.01 BTC

0.01 BTC

Transactions

- Each transaction is a transfer of money from inputs to outputs (many-to-many)



Inputs

1.1 BTC

1.5 BTC

Txn

1 BTC

1 BTC

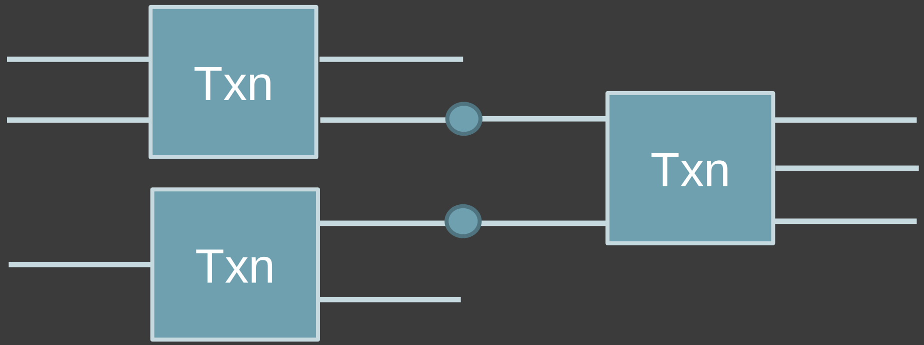
0.5 BTC

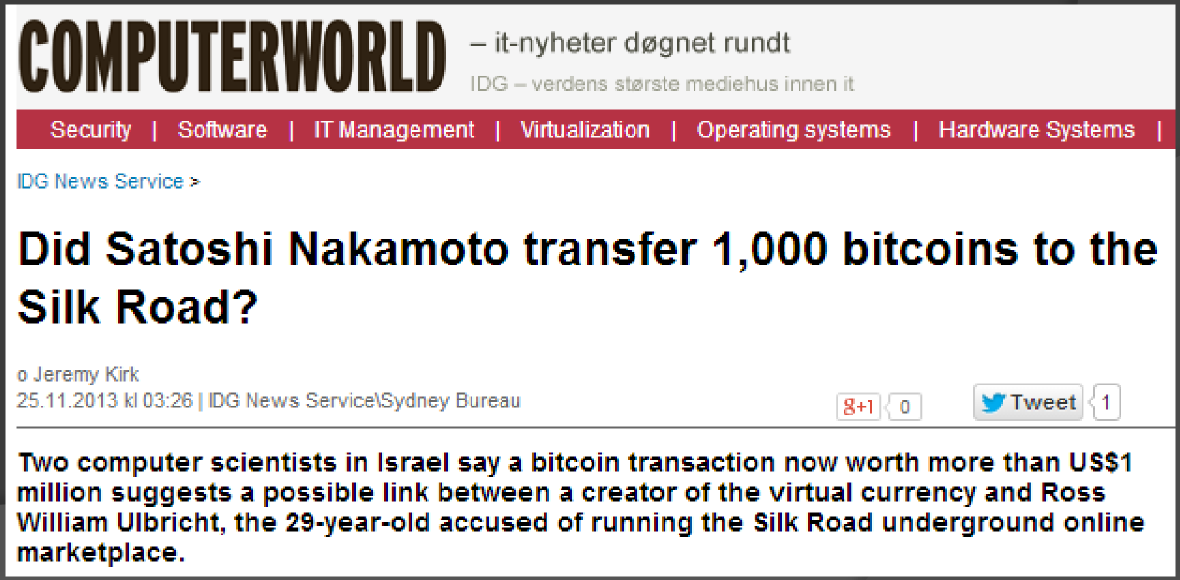
Outputs

(the fee is the difference between outputs and inputs)

A transaction is valid if and only if

- It contains all required signatures,
- every input matches a previous unspent output





COMPUTERWORLD – it-nyheter døgnet rundt

IDG – verdens største mediehus innen it

Security | Software | IT Management | Virtualization | Operating systems | Hardware Systems |

IDG News Service >

Did Satoshi Nakamoto transfer 1,000 bitcoins to the Silk Road?

o Jeremy Kirk
25.11.2013 kl 03:26 | IDG News Service\Sydney Bureau

Two computer scientists in Israel say a bitcoin transaction now worth more than US$1 million suggests a possible link between a creator of the virtual currency and Ross William Ulbricht, the 29-year-old accused of running the Silk Road underground online marketplace.

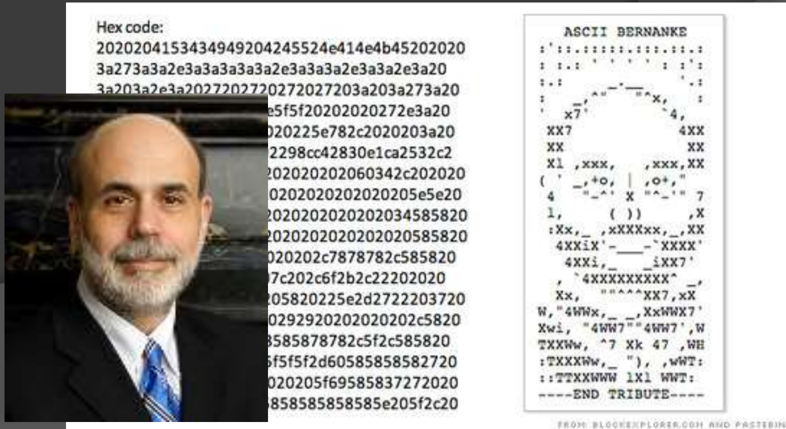
Transactions

- outputs specify amount and “script” for redeeming money.

```
OP_DUP OP_HASH160 5df3d323c10c8563e9086074c4bd94eab97b95a8
OP_EQUALVERIFY OP_CHECKSIG
```

- Inputs specify data for script to return “True”

- Some outputs cannot be redeemed.



Hex code:

```
20202041534349492042455524e414e4b45202020
3a273a3a2e3a3a3a3a3a2e3a3a3a2e3a3a2e3a20
3a203a2e3a20272027202720272027203a203a273a20
e5f5f20202020272e3a20
020225e782c2020203a20
2298cc42830e1ca2532c2
20202020060342c202020
0202020202020205e5e20
20202020202020034585820
20202020202020205585820
020202c7878782c585820
7c202c6f2b2c22202020
205820225e2d2722203720
0292920202020202c5820
3585878782c5f2c585820
5f5f5f2d6058585858582720
020205f69585837272020
858585858585e205f2c20
```

```
      ASCII BERNANKE
:'::.:::::.:::.::.:
: :.: ' ' ' ' : :':
:.:      _.__    '.:
:   _,^"   "^x,    :
'  x7'        `4,
 XX7            4XX
 XX              XX
 X1 ,xxx,   ,xxx,XX
( ' _,+o, | ,o+,"
 4   "-^' X "^-'" 7
 1,      ( ))     ,X
 :Xx,_ ,xXXXxx,_,XX
  4XXiX'-___-`XXXX'
   4XXi,_   _iXX7'
  , `4XXXXXXXXX^ _,
  Xx,  ""^^^XX7,xX
W,"4WWx,_ _,XxWWX7'
Xwi, "4WW7""4WW7',W
TXXWw, ^7 Xk 47 ,WH
:TXXXWw,_ "), ,wWT:
::TTXXWWW 1X1 WWT:
----END TRIBUTE----
```

FROM BLOCKEXPLORER.COM AND PASTEBIN

Scripts allow for much more…

- k out of n signatures
- Delayed payments
- Savings accounts

- P2P bets
- Derivatives
- Distributed exchanges

- Implemented on top of Bitcoin

Mastercoin

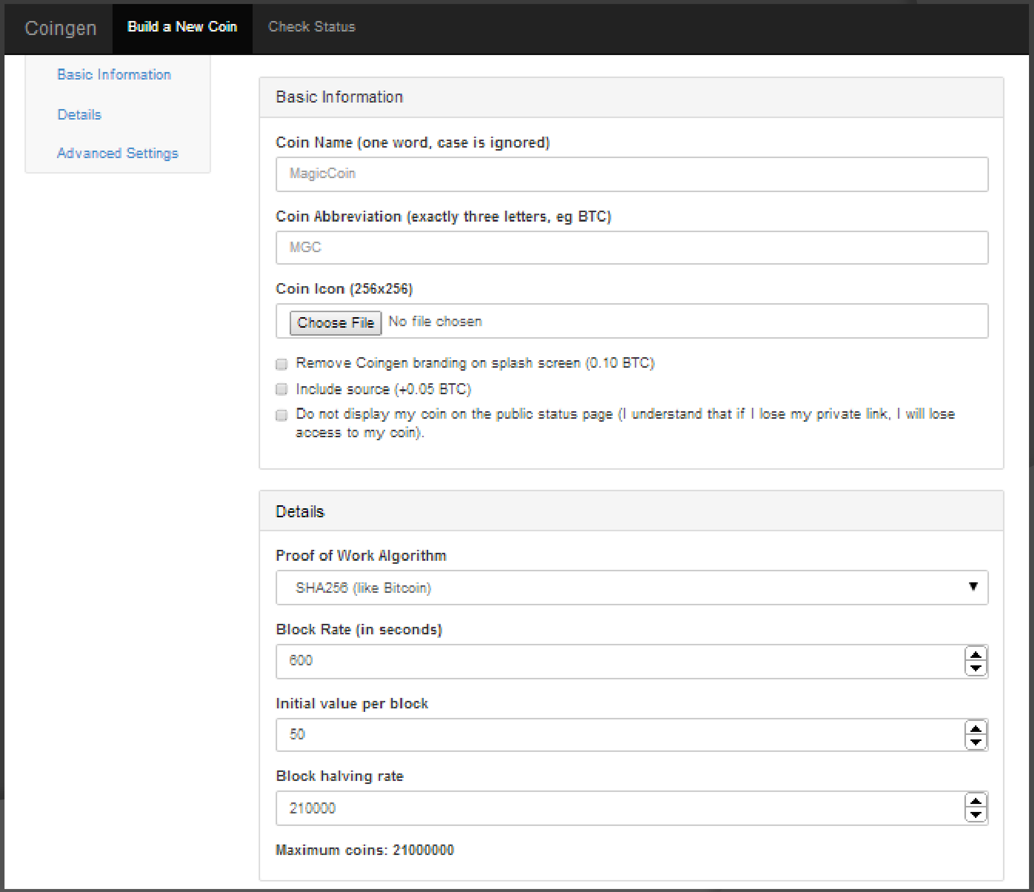
- or in alternative chains

ethereum

Modifications of the protocol

Altcoins

- Many Bitcoin clones



Basic Information

Coin Name (one word, case is ignored)

MagicCoin

Coin Abbreviation (exactly three letters, eg BTC)

MGC

Coin Icon (256x256)

Choose File No file chosen

□ Remove Coingen branding on splash screen (0.10 BTC)

□ Include source (+0.05 BTC)

□ Do not display my coin on the public status page (I understand that if I lose my private link, I will lose access to my coin).

Details

Proof of Work Algorithm

SHA256 (like Bitcoin)

Block Rate (in seconds)

600

Initial value per block

50

Block halving rate

210000

Maximum coins: 21000000

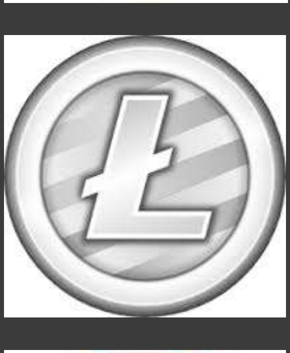
Zerocoin / Zerocash

[Ben-Sasson, Chiesa, Garman, Green, Miers, Tromer, and Virza]

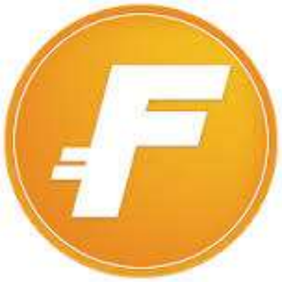
- Improved anonymity for Bitcoin using advanced cryptographic tools
  - zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs)
- Hides transaction origin, destination & amount.
- Most importantly: efficient implementation makes otherwise heavy crypto practical

Can Bitcoin Be Faster?

Block rate: one every 10 minutes



2.5 minutes



12 seconds

What is the effect of this? Why not go even faster?

Two related problems

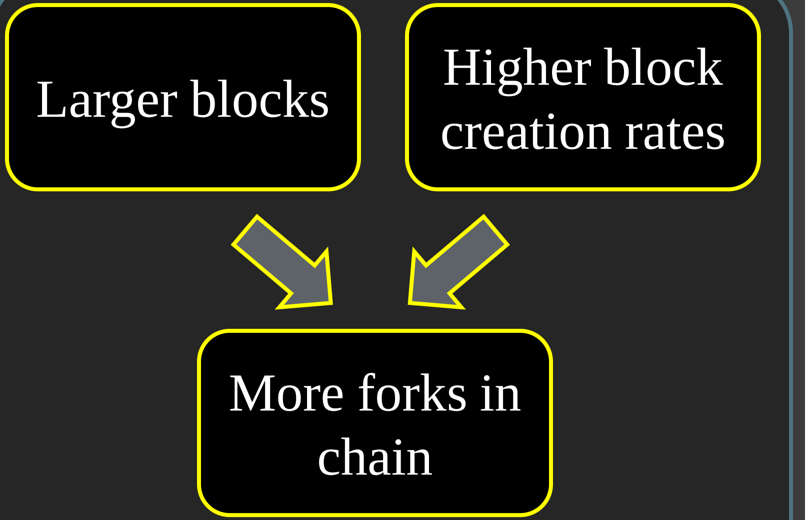
[Sompolinsky & Zohar]

A block every 10 minutes

- A Long wait for transaction confirmations

1MB per block (per 10 minutes)

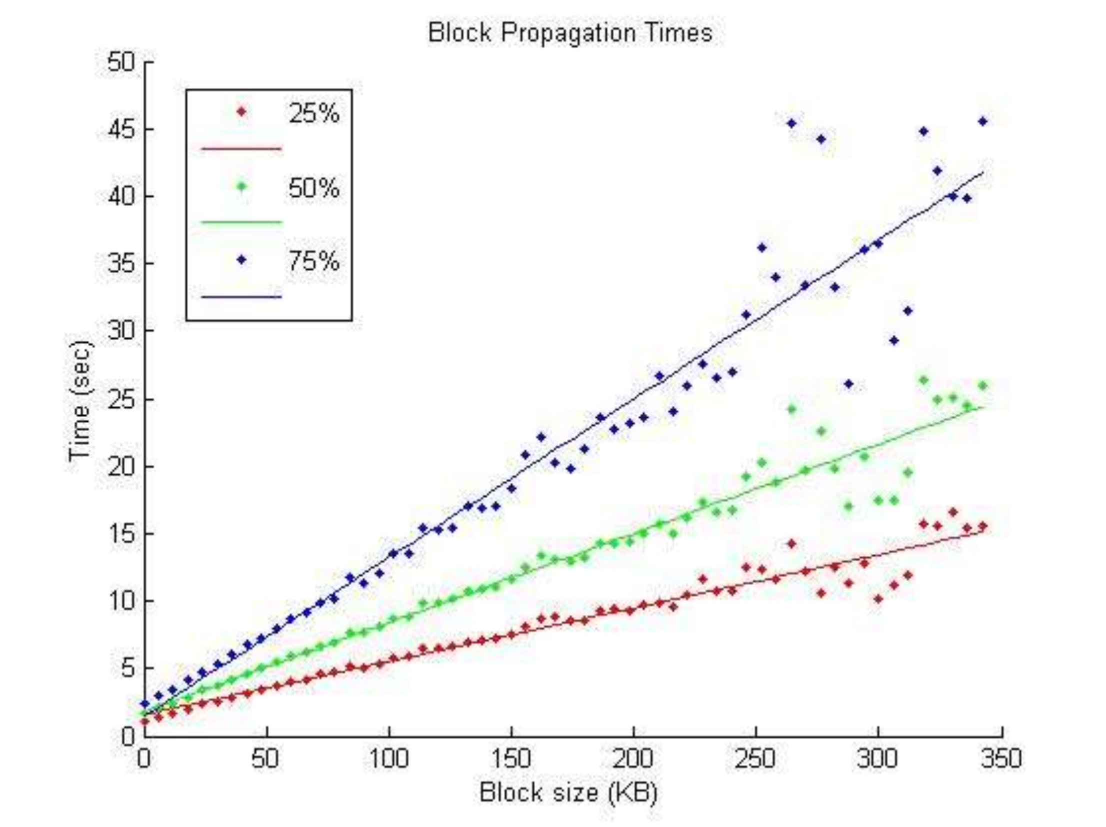
- A limit on number of transactions per second (3.3 TPS)



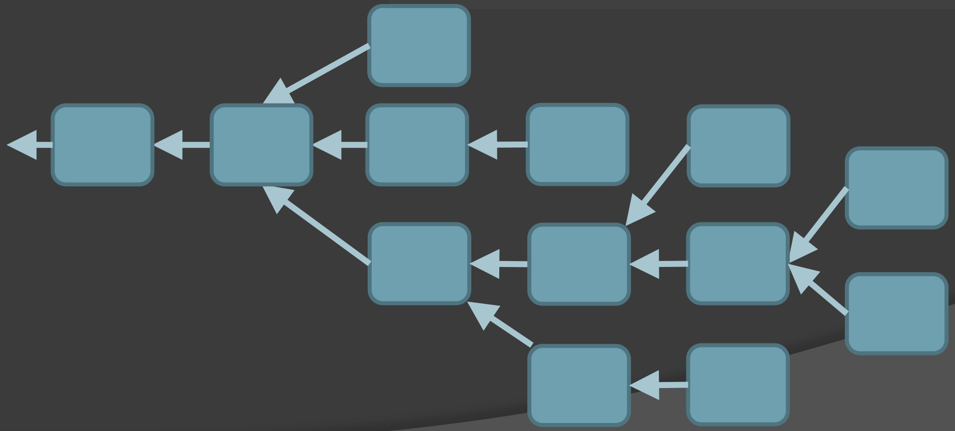
Larger blocks

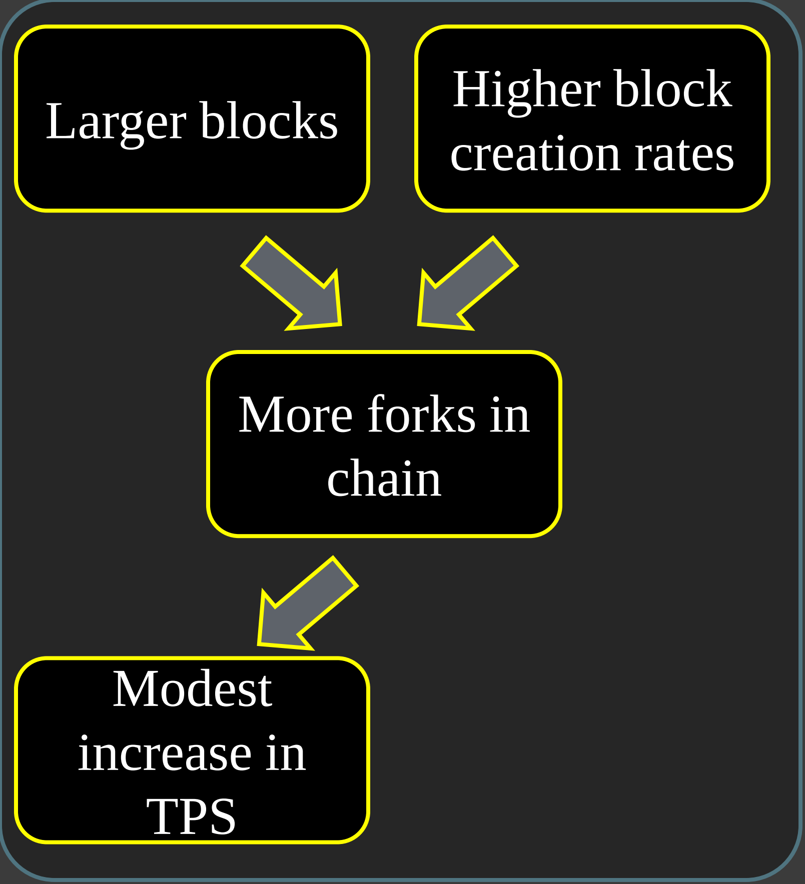
Higher block creation rates

More forks in chain



*Data generously shared by Decker & Wattenhofer



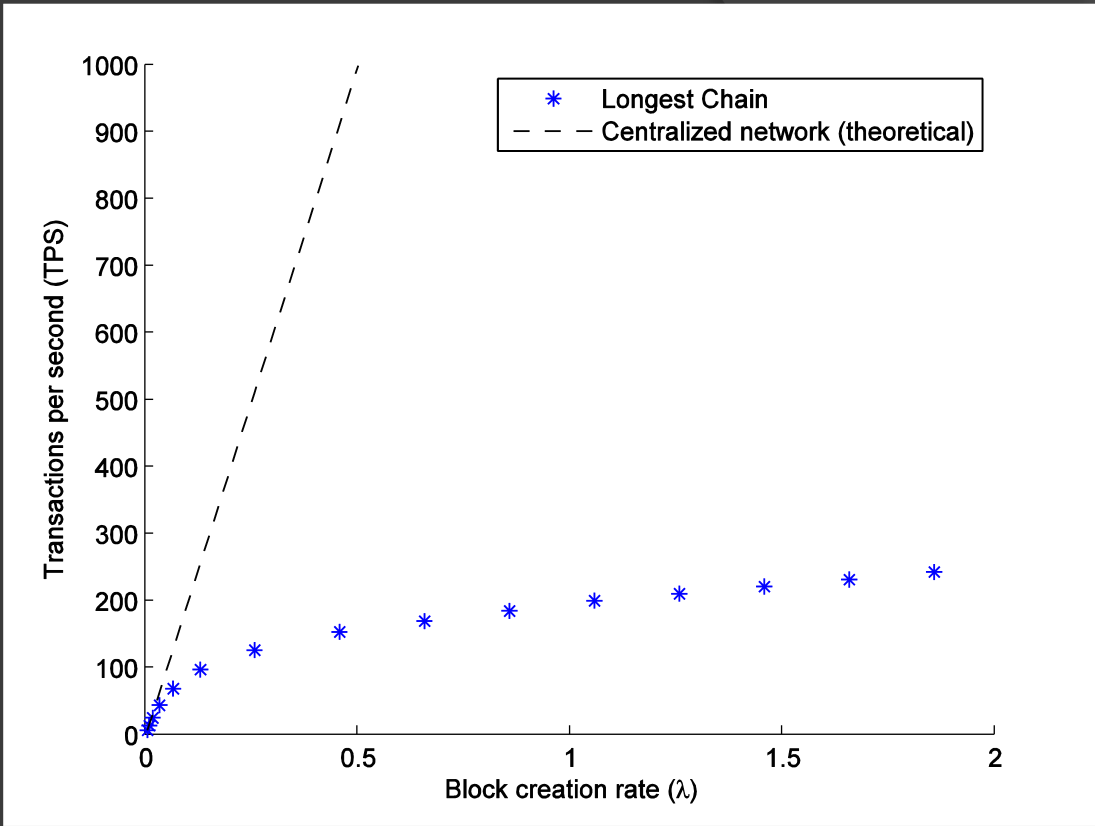


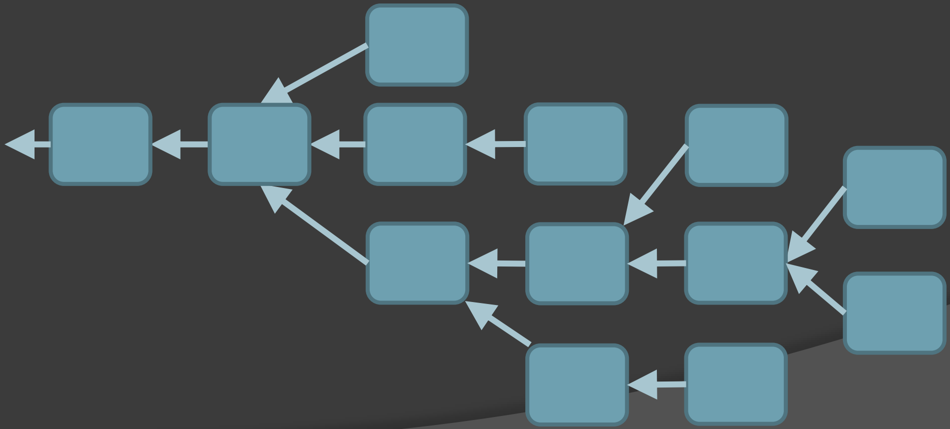
Larger blocks

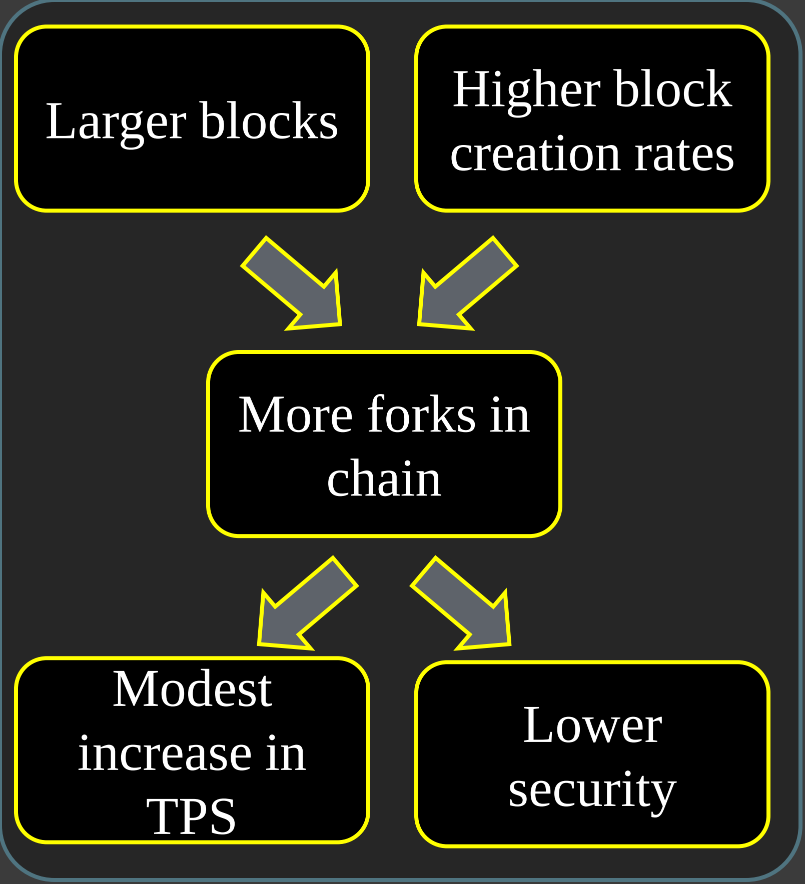
Higher block creation rates

More forks in chain

Modest increase in TPS







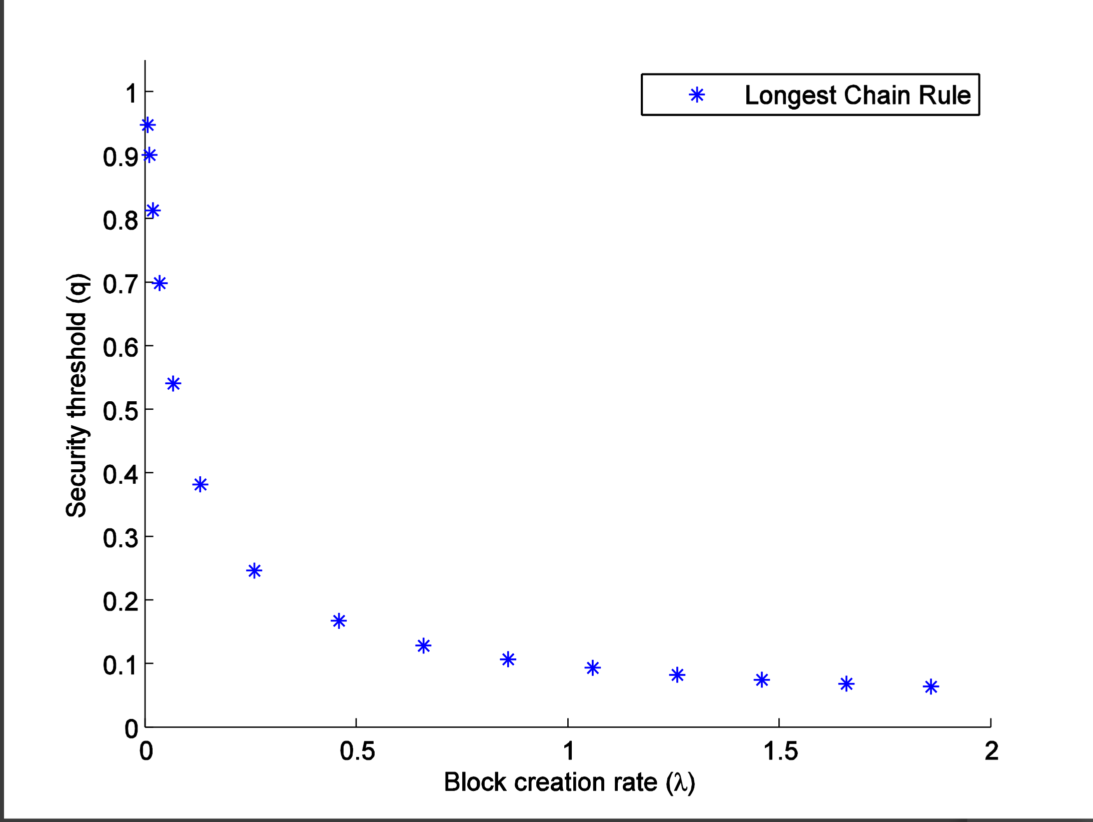
Larger blocks

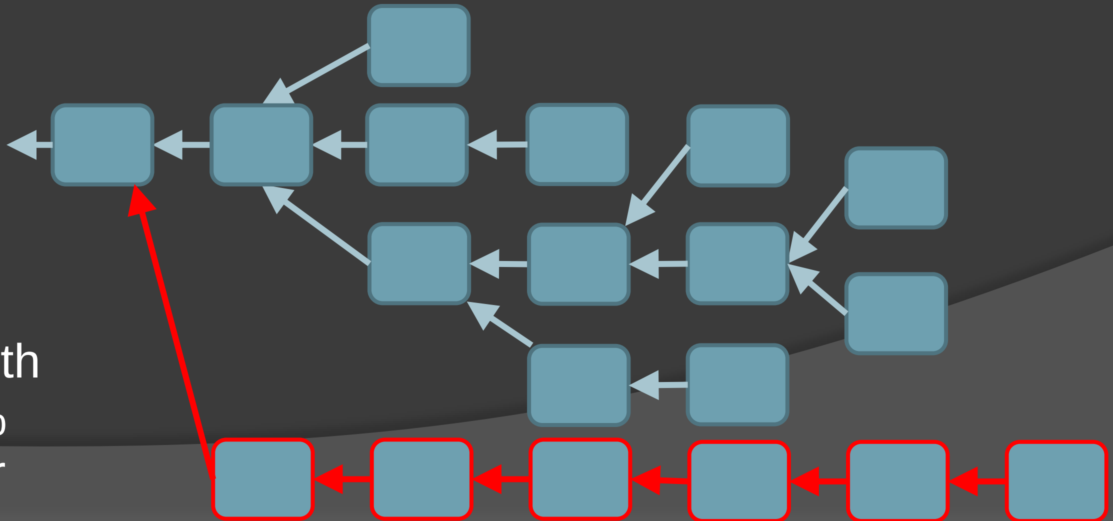
Higher block creation rates

More forks in chain

Modest increase in TPS

Lower security





50% attack with less than 50% of hash power

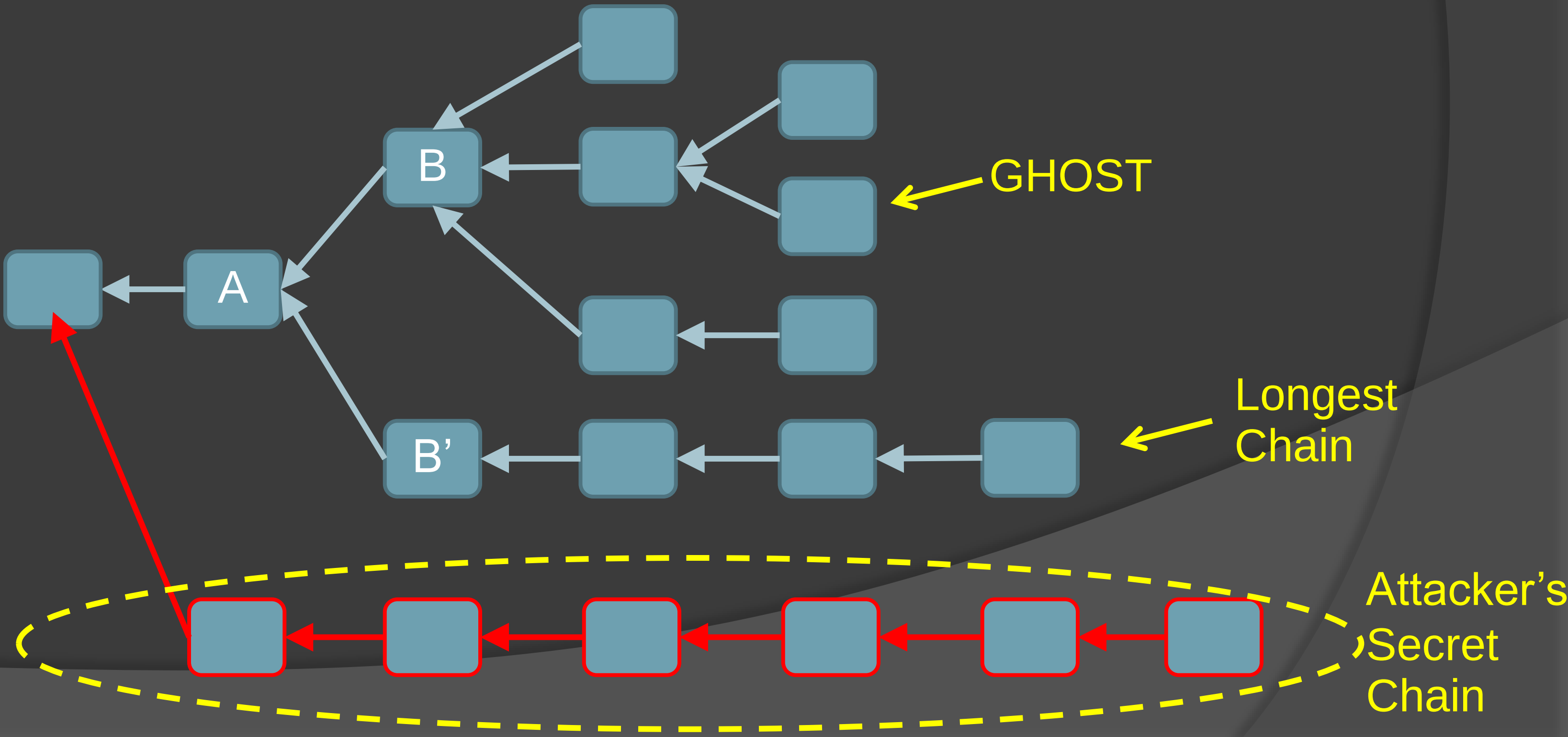
Greedy Heaviest Observed Sub-Tree (GHOST)

[Sompolinsky & Zohar]

An alternative chain selection rule (instead of “longest chain”)

- Begin at the “Genesis Block”
- At every split, pick the heaviest sub-tree.

Outcome: 50% attack only works with 50% of compute power.



The Pull Towards Centralization

- Advantage of large miners:
  - Economies of scale (e.g. datacenters in Iceland)
  - Block distribution to self not needed.
  - Attractive connections for other miners

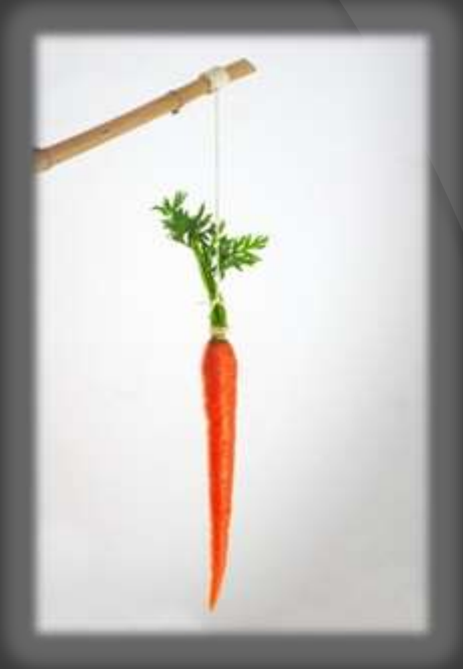
Outcome:

- Large miners gain more than proportional share.
- Drive small miners out of business.
- System becomes centralized.

- Gets worse at high block rates / large blocks

Incentives

Is the protocol
“incentive compatible”?



Two main issues found thus far:

1. Miners lack the incentive to flood transaction messages to others.

   On Bitcoin and Red Baloons [Babaioff, Dobzinsky, Oren & Zohar]

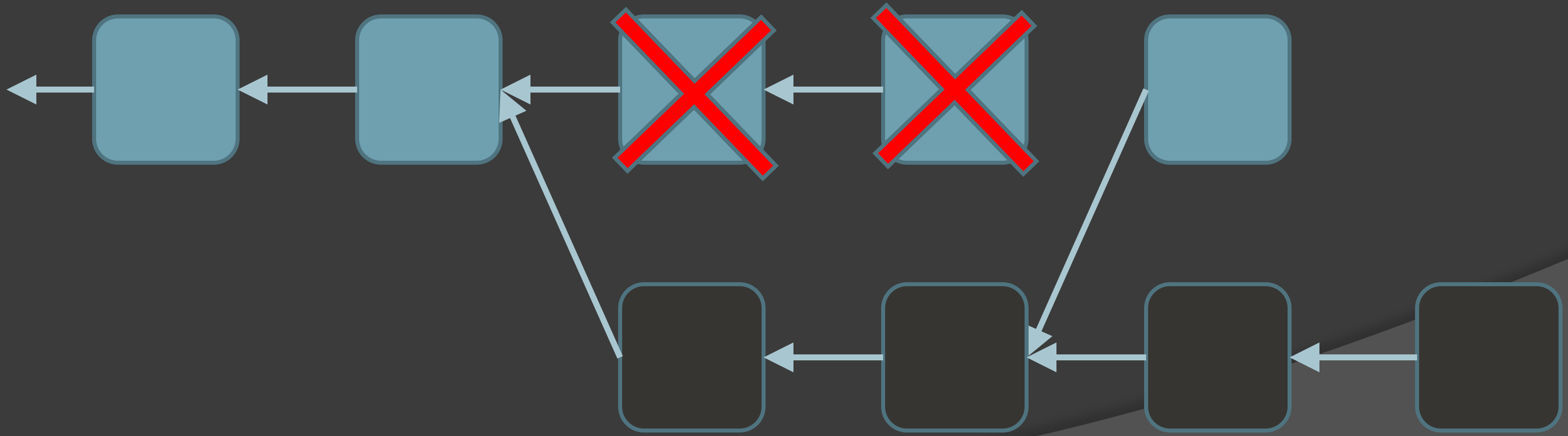
2. Miners do not necessarily want to mine on top of latest block or release their block instantly

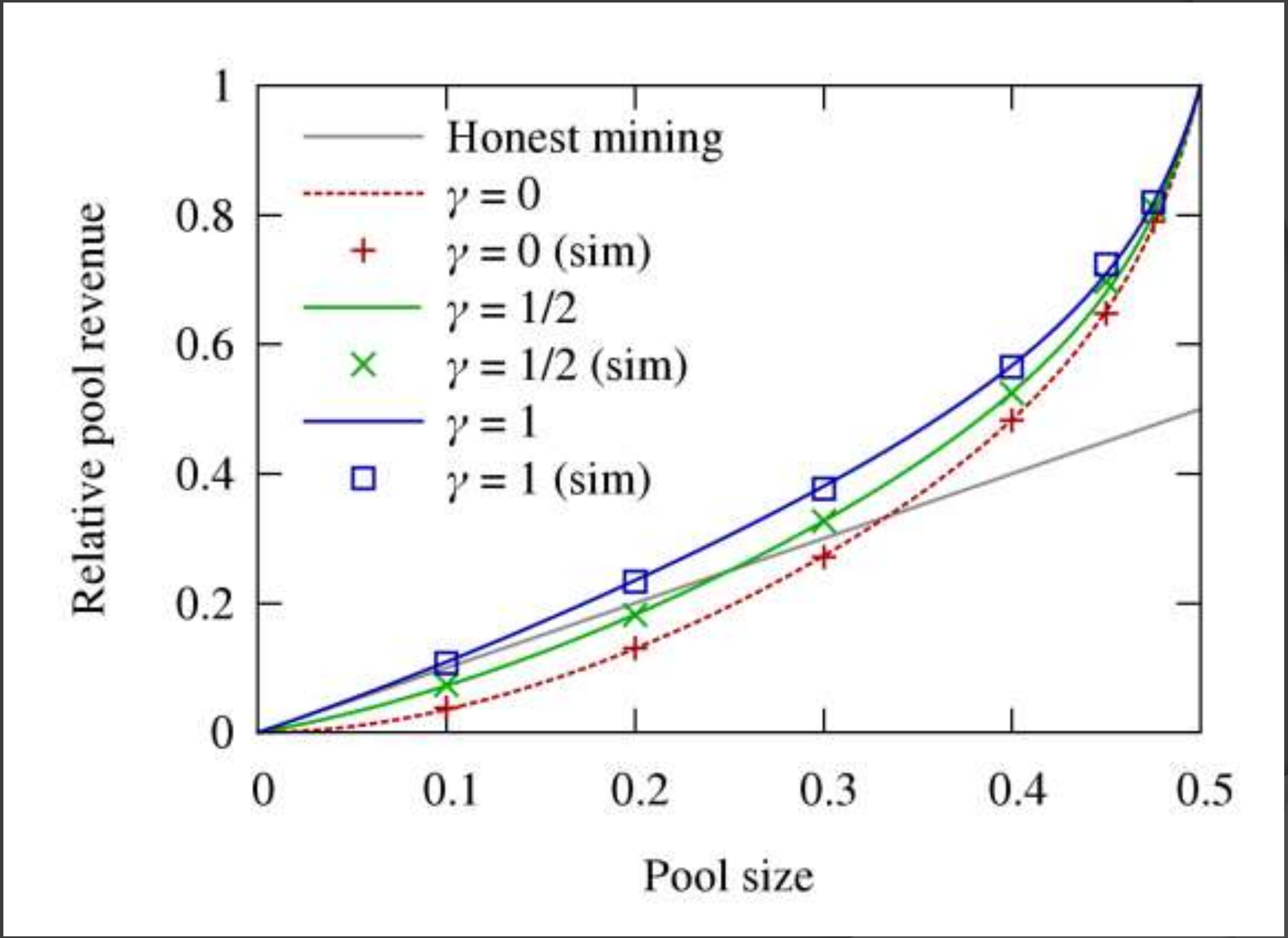
   “Majority is not Enough“ [Eyal & Sirer]

Block Withholding

[Ittay Eyal & Emin Gün Sirer]

Miners do not necessarily want to mine on top of latest block.



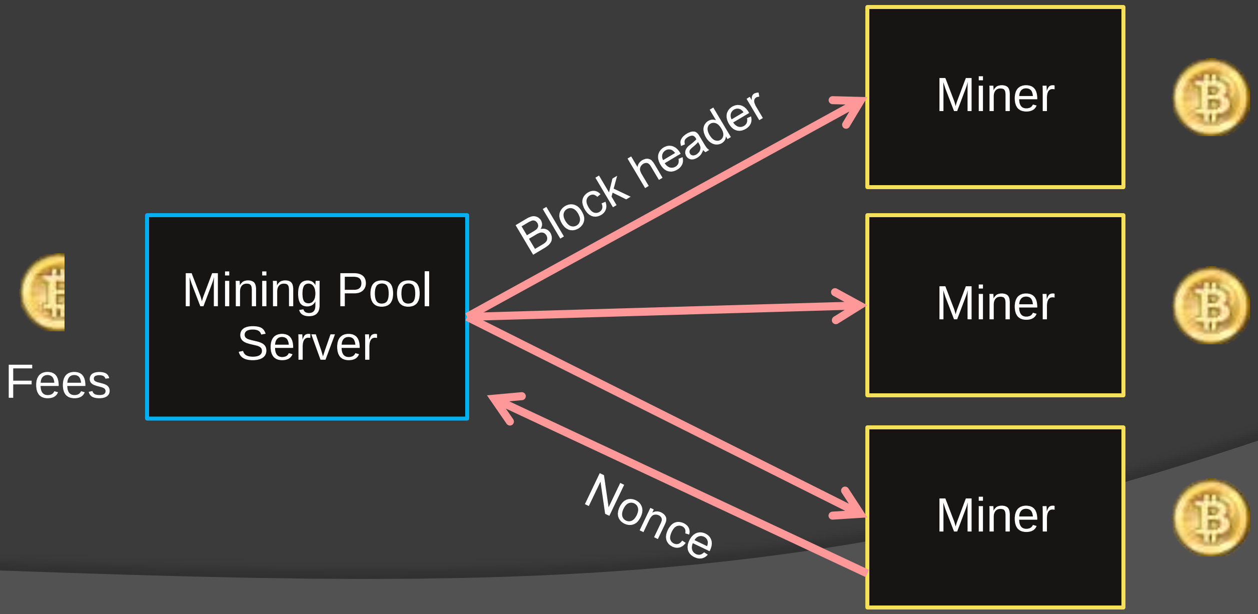


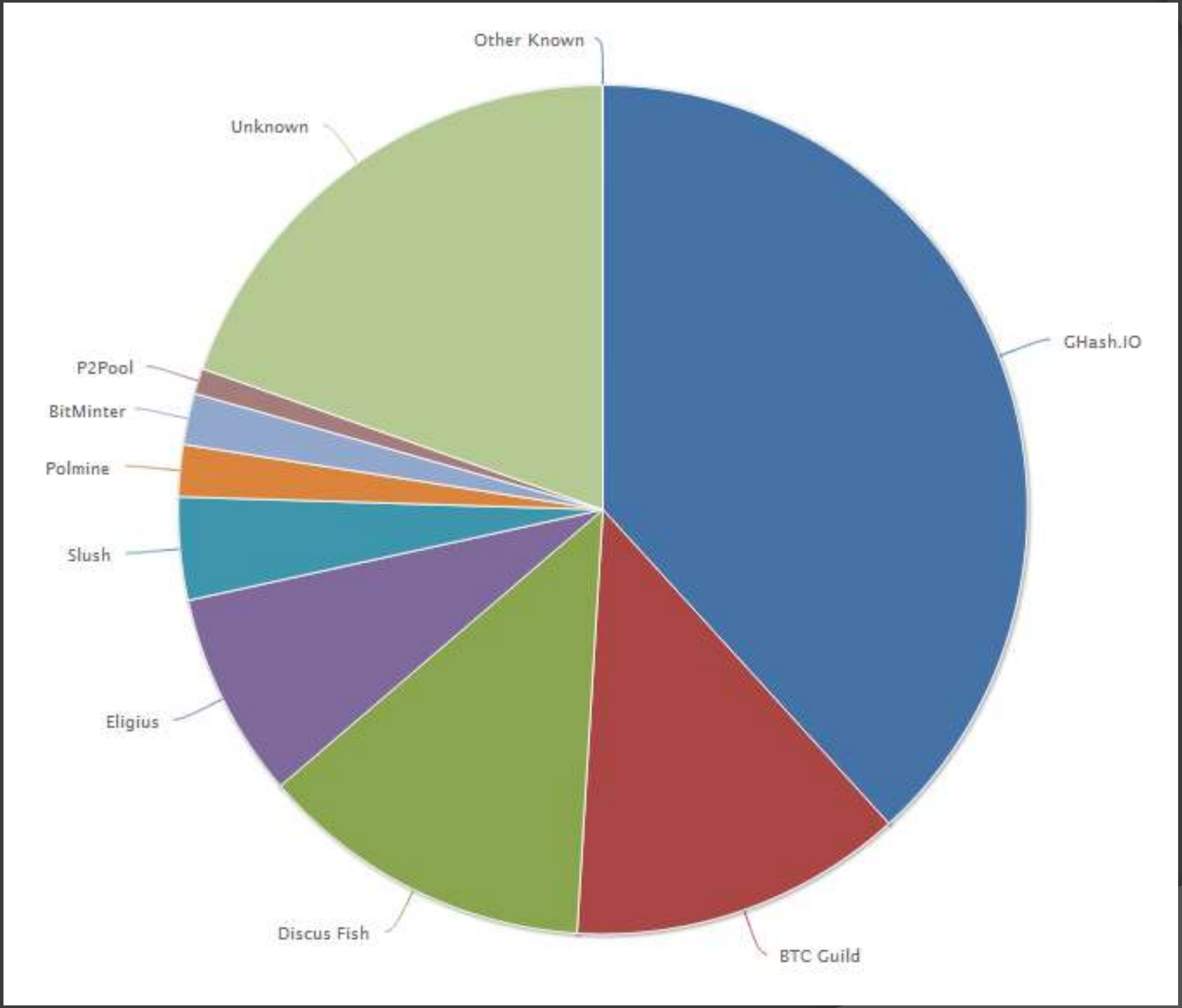
From: Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *arXiv preprint arXiv:1311.0243* (2013).

Mining Pools

Mining Pools

- Bitcoin mining is a high risk “lottery”
- Miners can join together to split profits and reduce risk





Hash rate distribution (from Blockchain.info)

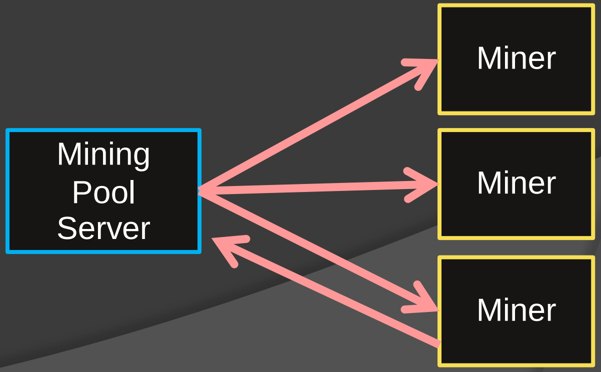
How (not) to split rewards

- Miners that contribute more should get higher reward.

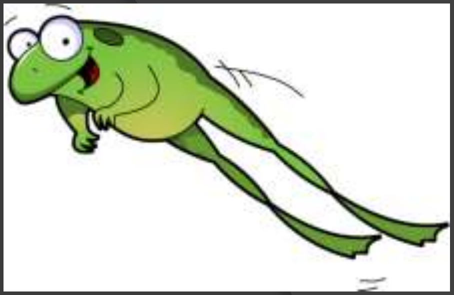
- Win: $\text{Hash(header)} < target$
- Get a share: $\text{Hash(header)} < k \cdot target$

Pay per share:

Split wins proportionately to # of shares contributed.



Pool Hopping



It is not known when a block will be created by the pool (a memoryless process).

- The first share may be worth a lot (if block found right after)
- The 50th share is already very “diluted”

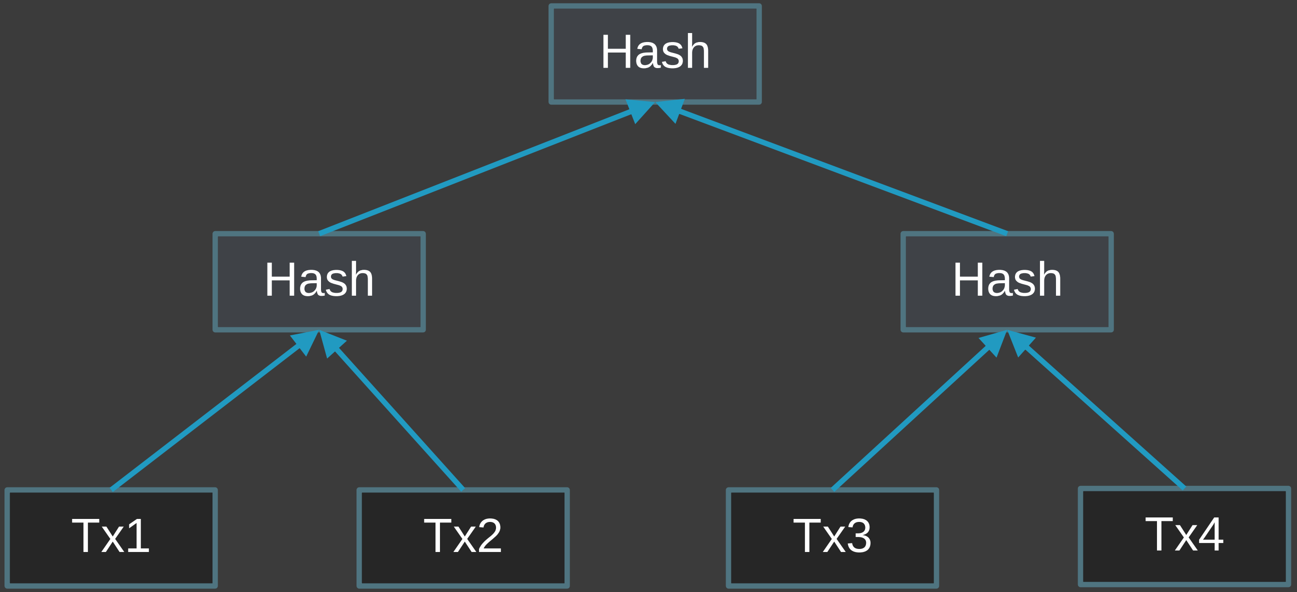
- Miners are better off switching to another pool / solo mining after several shares have been found.

Hop-proof reward schemes exist.

Explore tradeoff between risk to pool, risk to player and time. [Meni Rosenfeld]

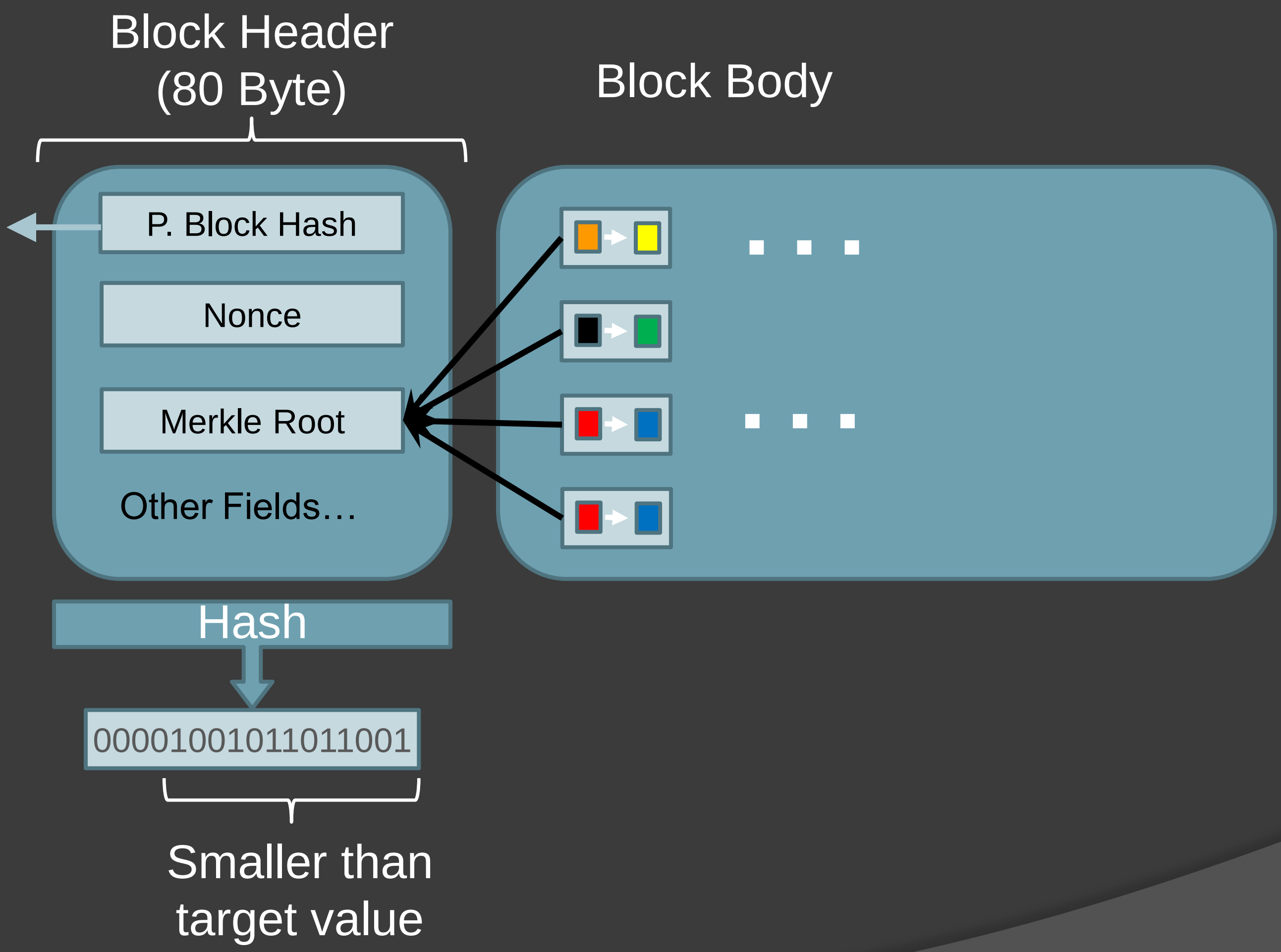
MORE ON STRUCTURE

More on Block Structure: Merkle Trees



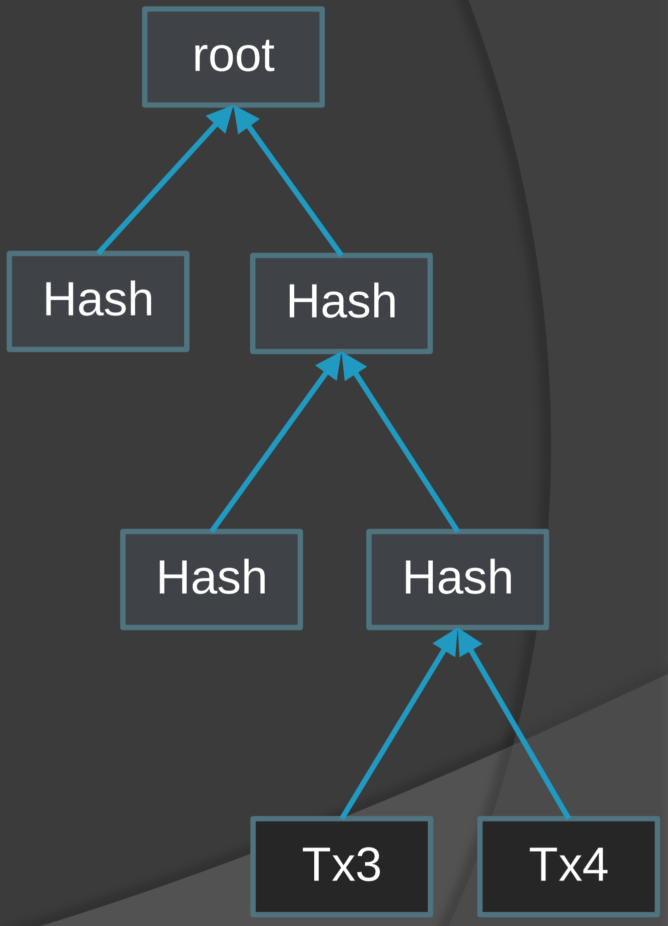
Specifying the root, is equivalent to committing to all transactions in the tree (unless we can easily find hash collisions)

Root of the Merkle tree is thus included in the block header.



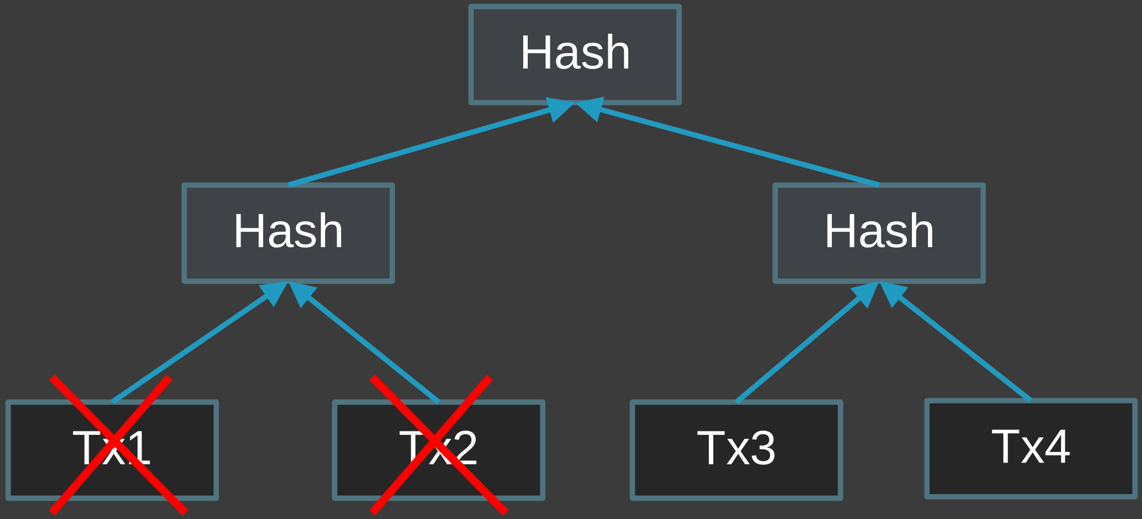
Light nodes

- Running a full Bitcoin node may be too expensive. (e.g. for smartphones)
- To prove that transaction occurred:
  - Download block headers and check nonce values, Merkle root
  - Request Merkle "branch" leading from some block to root

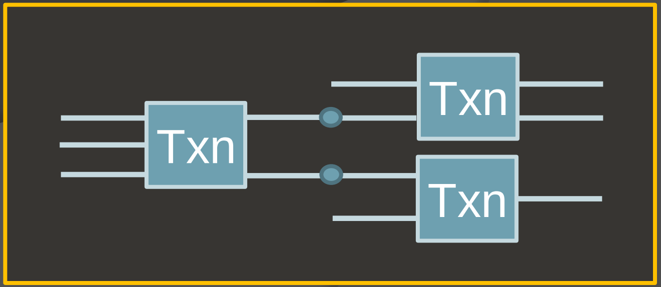


Saving space

- The same scheme allows full nodes to save space.

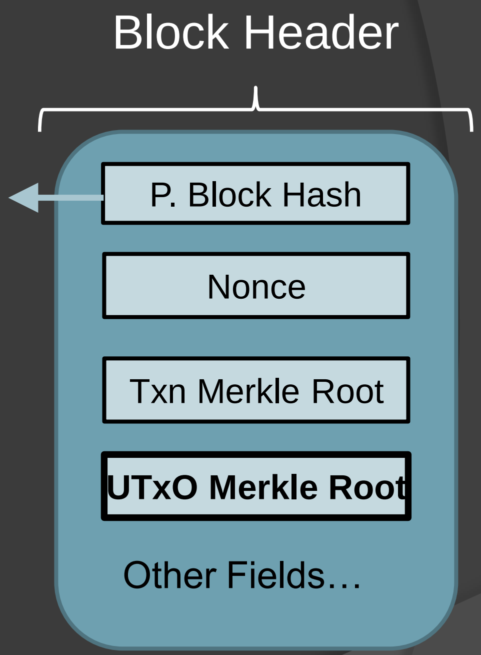


“Spent” transactions no longer needed



Unspent transaction outputs

- What about proving that money is in someone else's account? (Unspent output)
- Suggested modification: Include a Merkle root of unspent transactions in the header.
- Show a Merkle branch to the output.
- Allows for more space savings



Suggested Reading

- Bitcoin Wiki
- BitcoinTalk forums
- Bitcoin on Stack-Exchange

Some papers (in no particular order):

- Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
- Ben-Sasson, Eli, et al. "Zerocash: Decentralized anonymous payments from Bitcoin." *Security and Privacy (SP), 2014 IEEE Symposium on. IEEE*. 2014.
- Rosenfeld, Meni. "Analysis of hashrate-based double spending." (2012).
- Rosenfeld, Meni. "Analysis of Bitcoin Pooled Mining Reward Systems." *arXiv preprint arXiv:1112.4980* (2011).
- Babaioff, Moshe, et al. "On bitcoin and red balloons." *Proceedings of the EC* 2012.
- Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." *FC 2014*.
- Decker, Christian, and Roger Wattenhofer. "Information propagation in the bitcoin network." *IEEE P2P 2013*.
- Sompolinsky, Yonatan, and Aviv Zohar. "Accelerating Bitcoin's Transaction Processing.“ IACR eprint archive.
- Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013. 6-24.

Thank You!